

March 13, 2024

Elections Commission
c/o Hawai'i State Office of Elections
802 Lehua Avenue
Pearl City, Hawai'i 96782

Aloha, Commissioners,

**RE: SUPPORT FOR THE REAPPOINTMENT OF SCOTT T. NAGO AS
CHIEF ELECTION OFFICER**

This letter is to express my wholehearted support for the reappointment of Scott T. Nago as Chief Election Officer for the State of Hawai'i.

In my professional capacity as the County Clerk for the County of Kaua'i, I've worked closely with Mr. Nago since 2010 and found him to be highly knowledgeable and hardworking. He is a skilled manager and has assembled an exceptional staff of professional election officials who are committed to providing the voters of Hawai'i with open, honest, fair, secure, and transparent elections which are second to none.

During these contentious times, Mr. Nago's experience, and principled and committed leadership is needed more than ever so I urge Commissioners to support his reappointment as Hawai'i's Chief Election Officer.

Thank you for this opportunity to express my wholehearted support for the reappointment of Scott T. Nago as Hawai'i's Chief Election Officer.

Sincerely,

A handwritten signature in black ink, consisting of a large, stylized 'J' followed by several loops and a long horizontal line extending to the right.

JADE K. FOUNTAIN-TANIGAWA

March 17, 2024

Elections Commission
802 Lehua Avenue
Pearl City, Hawaii 96782

Dear Chair Curtis and members of the Elections Commission:

My name is Aulii Tenn. I serve as the Counting Center Section Head at the Office of Election, and I appreciate the opportunity to submit written testimony in my individual capacity in strong support of reappointing Scott Nago to the position of Chief Election Officer.

I have worked with Scott since 2012 and during this time, he has become my mentor. Over Scott's most recent term as Chief Election Officer, since 2020, he led the office through the transition and implementation of elections by mail, and through the COVID-19 pandemic. Scott leads by example. He does not have an ego that keeps him sitting behind a desk; he understands and is determined that the task is to conduct the election. I found working through the COVID-19 pandemic to be very stressful knowing that we would have to ensure our health and the health of the volunteers and other agencies we work with. It also happened to be the first year of statewide elections by mail resulting in a shift in dynamics and responsibilities. Scott is a fair, empathetic, and pragmatic leader. He is available to talk through the stresses and he continues to inspire me. He also emphasizes doing the right thing by focusing on the conduct of the election. Scott has taught me professionalism, personal growth, and of course – how to run elections.

Elections are like the seat of a 3-legged stool, with voters, candidates, and administration being the legs. Each leg is required to function. Specifically, every election is impacted by the interest and engagement of voters and the candidates running for office, while the Office of Elections is part of the administration providing services and the mechanics of voting. The mission of the Office of Elections is to provide secure, accessible, and convenient election services to all citizens statewide. The responsibilities of the Office of Elections are the printing and counting of ballots and voter education.

The change to elections by mail has been the most significant transition in Hawaii's election system. Before elections by mail, Hawaii provided for no-excuse absentee voting since 1993, and permanent absentee ballot requests since 2008. Before voting by mail started in 2020, the number of ballots cast by mail increased by 61.6% for the primary election and 57.4% for the general election from 2010 to 2018. In turn, the number of voters who had decided to vote in person decreased by 37.3% for the primary election, and 27.7% for the general election at early walk in voting locations; and 34.3% for the primary election, and 21.2% for the general election at polling places.

In the elections Scott has administered, voter registration continues to increase and there has been growth in the number of voters casting a ballot. On average, between 2010 and 2022, voter registration has grown by 3.8% and the number of voters casting a ballot has increased by 4.2%. I also think that it is significant that as Chief Election Officer, Scott has administered 7 of the 10 elections with the greatest number of voters. Of those 7 elections, 3 were conducted by mail. I also think it is worth noting that looking specifically at primary elections, the 2022 Primary Election had the second highest number of voters, only behind the 2020 Primary Election.

Scott is integral to the conduct of elections and is the leader of the Office of Elections. His management style is to encourage and challenge ideas and to support teamwork. He has taught me the interconnectivity required to make the office function and emphasizes how one decision impacts other tasks and events. I am also grateful for how Scott takes the time to listen to my opinions, and in turn, provides advice and serves as a voice of reason for the circumstances. The skills I have learned from him I try to apply to my life. I appreciate Scott's dedication, integrity, and willingness to help – all of which are important to his position as Chief Election Officer.

Scott will continue to be a steadfast leader to ensure secure, accessible, and convenient elections for the citizens of Hawaii and improve the administration of elections.

Sincerely,



Aulii Tenn

March 16, 2024

Mr. Michael Curtis, Chairperson
Members of the Elections Commission
Elections Commission
c/o Office of Elections
802 Lehua Avenue
Pearl City, Hawaii 96782

Dear Chair Curtis and Members of the Elections Commission:

I'm writing in strong support of Mr. Scott Nago's reappointment as Chief Election Officer for the State of Hawaii. I started in the Office of Elections in 2010, and during my time there, Mr. Nago has provided me with the support, resources, and leadership to accomplish my duties.

Mr. Nago has always been available to discuss any questions I have. I appreciate that he not only takes the time to explain the reasoning behind procedures but also fosters an environment of open dialog and encourages sharing new ideas. This not only provides a better understanding of the election process but also promotes critical thinking and innovation, enabling us to improve the operations of elections.

We are very fortunate to have a Chief Election Officer with institutional knowledge about the election process. Mr. Nago's years of experience not only bring stability to the office but also instill a sense of confidence in the team, knowing that we are led by someone who has a deep understanding of our work and its challenges.

Thank you for considering reappointing Mr. Scott Nago as Chief Election Officer.

Sincerely,

A handwritten signature in black ink, appearing to read 'Kristen Uyeda', written in a cursive style.

Kristen Uyeda

From: [Claire Ortega](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Oppose Reinstating Scott Nago
Date: Saturday, March 16, 2024 4:14:54 PM

I oppose reinstating of Scott Nago as Chief Elections Officer. There has not been a public review of his performance over the years. HRS 11-7.5(6) states the public's right of review.

There are significant grievances of election irregularities and fraud under his watch. Scott Nago has actively worked against election integrity and transparency.

In the 2022 Primary and General elections Scott Nago and the Office of Elections did not follow the HRS 16-42 law and audit the actual "voter verifiable paper audit trail." When citizen's and political parties tried to compel the Office of Elections to follow the 16-42 audit law, Scott Nago chose to introduce legislation to eliminate the audits entirely. This was a willful act by Scot Nago to make our Hawaii Elections less secure and transparent and it should disqualify him from his position as Chief Election Officer.

In addition, Scott Nago and the Office of Elections completely ignored the serious issues the Kauai Elections division has with ballot chain of custody which also should disqualify him. Hawaii citizens need a chief Elections Officer that will make our elections more accountable and transparent not less.

Thank you,
Claire Ortega

From: [Steve O'Neill](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Scott Nago
Date: Saturday, March 16, 2024 5:03:14 PM

Elections Board

I oppose reinstating of Scott Nago as Chief Elections Officer. There has not been a public review of his performance over the years. HRS 11-7.5(6) states the public's right of review.

There are significant grievances of election irregularities and fraud under his watch. Scott Nago has actively worked against election integrity and transparency.

In the 2022 Primary and General elections Scott Nago and the Office of Elections did not follow the HRS

16-42 law and audit the actual "voter verifiable paper audit trail." When citizen's and political parties tried to compel the Office of Elections to follow the 16-42 audit law, Scott Nago chose to introduce legislation to eliminate the audits entirely. This was a willful act by Scot Nago to make our Hawaii Elections less secure and transparent and it should disqualify him from his position as Chief Election Officer.

In addition, Scott Nago and the Office of Elections completely ignored the serious issues the Kauai Elections division has with ballot chain of custody which also should disqualify him. Hawaii citizens need a chief Elections Officer that will make our elections more accountable and transparent not less.

Thank you for your time.

Regards, Steve and Linda O'Neill

Testimony for Elections Commission Meeting

Tuesday, March 19, 2024, 1:30 p.m.

Submitted by Judith Mills Wong, League of Women Voters of Hawaii

The League of Women Voters of Hawaii is a non-partisan organization that builds citizen participation in the democratic process. We work to protect and expand voting rights and ensure everyone is represented in our democracy. Our volunteer members throughout Hawaii assist with voter registration, vote counting and elections observation.

Thanks to all members of the Elections Commission for their service to Hawaii's citizens. This certainly includes the Chair of the Commission, whom we acknowledge and appreciate for his success in preventing anyone from willfully disrupting the conduct of Commission meetings.

Your past two meetings have been dominated by complaints from many sources. It is true that one of the legal duties of the Elections Commission is to investigate and hold hearings to receive evidence of any election violations and complaints. The League of Women Voters supports the public's right to make a complaint to the Elections Commission, but we strongly oppose rumors and misinformation that might undermine the public's confidence in Hawaii's elections.

Many of the comments and complaints voiced in the last meeting conflate the activities of the election process. Complaints that are under the purview of the Chief Elections Officer and his staff, should be addressed to this commission. Complaints regarding the responsibilities of the various County Clerks should be addressed to the appropriate County Council. Issues that are mandated by the legislature cannot be addressed by the Office of Elections and should not be considered in the evaluation of that office's performance.

Our members have actively participated in both County and State activities, particularly pre-testing voting machines, tabulating votes, recounts, and audits. Because of our experience as firsthand election observers, we have the utmost trust that our County Clerks will continue to maintain and update voter registration records so that all eligible voters will be able to vote. Our experience leads us to believe that County Clerks will reliably mail out and collect ballots, verify ballots received, screen envelope signatures for registered voters only, select places of deposit in their County, and operate voter service centers in the County. If/when a problem is identified within the responsibility of the County Clerk's office, this problem should be addressed and corrected promptly. Our experience with the State Office of Elections gives us confidence that that office will continue to certify candidates, design and print all ballots statewide, count all votes cast and conduct recounts and audits as appropriate. If/when a problem is identified within the purview of the Office of Elections, it should be addressed and corrected promptly.

Recently your Commission evaluated the performance of Hawaii's Chief Election Officer. The League takes no position on personnel matters involving public employees. All elections officials need to constantly review procedures and make improvements where necessary, but personal attacks against any employees are dangerous to our democracy. The Chief Elections Officer and staff of the Office of Elections coordinate and run a complex and important process. It is vital that these functions be handled with the upmost care. For that reason, the Chief Elections Officer must be experienced and professional. The election process contains a myriad of steps, each of which is vital to the conduct of fair elections. The process is extremely complicated and proper administration is not a task untrained personnel. Our experience with the Office of Elections and the current Chief elections Officer have found them to be competent and professional.

We can see plans are well underway for this year's primary and general elections. Let's move ahead to empower voters and make democracy work through voter education and modern elections administration. The League will strongly support elections officials in this effort, particularly by serving as official Election Observers. Observers are needed to provide independent oversight of our elections, and we urge the public to consider this volunteer opportunity.

After decades of trying, the League is pleased to see stronger statewide voter education in Hawaii, because of the 2023 passage of Act 115 that requires the Office of Elections to prepare a digital voter information guide; post the guide on its website in compliance with certain accessibility standards; and mail each ballot with a notice that states a voter information guide may be found on its website. The public is entitled to know a candidate's qualifications and a candidate's position on issues affecting their district, so we hope all candidates will submit statements. Also, the Attorney General and county corporation counsels are required to draft explanations of proposed constitutional or charter amendment ballot questions and translate them into certain languages for purposes of the digital voter information guide.

Speaking of accessibility, we are pleased to see that the Statewide Accessibility Needs Committee has been reviewing software that will be used by 2024 election voters with accessibility needs. We also commend the Maui County Clerk for an excellent voter information website that highlights Voter Accessibility. Maui County and the state Office of Elections are working to help displaced Lahaina voters receive their mail-in ballots ahead of the August primary, encouraging voters to update their mailing address. All eligible voters should be able to vote!

Thank you for the opportunity to submit testimony.

From: [Gail Smith](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] EC Mtg. 3/20/2024 @ 1:30 pm
Date: Monday, March 18, 2024 10:18:56 AM

Aloha Mike Curtis, Elections Commission Chair,

I am in opposition to Scott Nago's reappointment as CEO of the Office of Elections because of a few observations I have made as an Official Observer from the 2022 Primary and General Elections on Kauai. I am not able to attend your meeting but will submit testimony. Sorry it may be late.

1. Voting roles were not updated to remove single voter listings with multiple names and addresses, people who have moved, people who were ineligible to vote because of health conditions, and of deceased, etc. During the signature verification process, many ballots could not be "cured". Lots of wasted time and effort for the workers.
2. The voting ballot instructions were not followed during the audit/counting of votes. The instructions specifically stated that "You MUST select ONE political preference from the box above for your votes to count." The observers conducting the initial audit were confused and needed to recount about 3 times. Instructions should match the counting process. During the counting, a Hart worker stated that the instruction could be overlooked if the voter voted for one political party only. That was during the Primary Election.
3. Post election auditing consisted of paper ballot "images" being tallied. When questioned about using the actual paper ballots which were mixed up in district "batches", they needed to be recovered and counted. The amount counted was not for an entire precinct which would follow the 10% rule. It was done only for the tallied ballot images. The actual ballots were not kept in the order of Precincts received from the Elections Office but mixed up into 3 Districts. This was for the Primary election. The actual paper ballots would not have been counted if it was not requested by an official observer.
4. Per General Election auditing, it was easier to access paper ballots because prior to opening the ballots, the observers noticed the same method of grouping into districts was going to occur, and requested that the ballots be ORGANIZED AS RECEIVED. That is, by the 16 individual districts/precincts. The audit with the paper ballots took place because it was requested by the official observers. It was for one race each per precinct of 2 precincts. If not requested, the audit would be using only ballot images.

If mail-in ballots are the answer to voting in person with paper ballots in individual precincts, why does it take so much longer with so much confusion, time and effort on everyone, especially the Office of Elections workers? Why are we wasting time and effort on a process that does not result in clean and trustworthy elections?

I oppose the reappointment of Scott Nago as CEO.

Respectively submitted,
Gail Smith

This March 2024 Election Commission testimony is being presented in addition to the information included in your supplemental meeting packet relating to the inefficiency of Hawaii vote-by-mail elections and regarding the reappointment of the chief election officer.

As the commission may recall, during your February 20th EC meeting, the commission had a discussion about the implementation of ERIC and which the Chief Election Officer participated, and wherein the commission subsequently voted in opposition to the implementation of ERIC.

Following that vote, the Chair stated that "The commission is making a statement that we oppose ERIC."

Three weeks later, On Friday March 15 during the House Committee on Judiciary & Hawaiian Affairs hearing on SB 2240 SD2 and regarding the implementation of ERIC, your Chief Election Officer (Mr Nago) submitted written testimony and testified to Chair Tarnas that the "Office of Elections stands on its written testimony" (in support of ERIC).

In his written testimony, Mr Nago never acknowledged nor noted the decision by the Elections Commission opposing ERIC that occurred during the February Election Commission meeting. (See Enclosure (1))

Despite the Elections Commission decision and vote during the February Elections Commission meeting, there was also no testimony submitted by the Election Commission in opposition to SB 2240 SD2.

Fifty-five testimonies were submitted in opposition to ERIC.

As you know, per HRS 11-1.6(a) the chief election officer is appointed by the elections commission, and per HRS 11-7.5(7) the duties of the election commission are to "advise the chief election officer on matters relating to elections."

How is it possible that the despite the Elections Commission opposition to ERIC, and the advice you gave to Mr Nago in opposition to the implementation of ERIC, that Mr Nago then submits written and verbal testimony in support of ERIC and the system that the commission voted in opposition to implement?

Does the Election Commission consent to Mr Nago's testimony to the House Committee on Judiciary & Hawaiian Affairs in support of an elections system that the commission voted against implementing?

Does the Election Commission consent to Mr Nago's intentional disregard and insubordination to the "advice" provided by the commission?

When is the commission going to act like the boss instead of letting Mr Nago dictate the conduct of elections that are being actively questioned and challenged by the people, and even those being opposed by the Elections Commission?

As you likely know, two votes were held during the February Election Commission meeting and Mr Nagos reappointment failed during both. Mr Nagos reappointment failed with a tie vote to "not reappoint" and also through a subsequent failed vote to "reappoint" him as the Chief Election Officer.

When is the Elections Commission going to take responsibility for the oath you took as commissioners and the duties entrusted to you by the people?

Last, I again respectfully request that the commission investigate how the Office of Elections implementation of vote-by-mail has met their mission and demonstrated efficiency, encouraged participation, or promoted participation in Hawaii's elections. (See Enclosure (2)).

Thank you for the opportunity to address the commission.

V/R, Doug Pasnik, ARR



**STATE OF HAWAII
OFFICE OF ELECTIONS**

802 LEHUA AVENUE
PEARL CITY, HAWAII 96782
elections.hawaii.gov

SCOTT T. NAGO
CHIEF ELECTION OFFICER

TESTIMONY OF THE

CHIEF ELECTION OFFICER, OFFICE OF ELECTIONS

TO THE HOUSE COMMITTEE ON JUDICIARY AND HAWAIIAN AFFAIRS

ON SENATE BILL NO. 2240, SD 2

RELATING TO ELECTIONS

March 15, 2024

Chair Tarnas and members of the House Committee on Judiciary and Hawaiian Affairs, thank you for the opportunity to testify in support of Senate Bill No. 2240, SD 2. This bill requires the Office of Elections to file an application with Electronic Registration Information Center, Inc. (ERIC), by June 30, 2025, for the State to be admitted as a member of the organization; requires the Office of Elections to share with each county the information and services made available by ERIC pursuant to the State's membership agreement with the organization; requires the Office of Elections and each county office that administers elections to use information and services made available by ERIC to verify their respective voter registration rolls; and makes an appropriation.

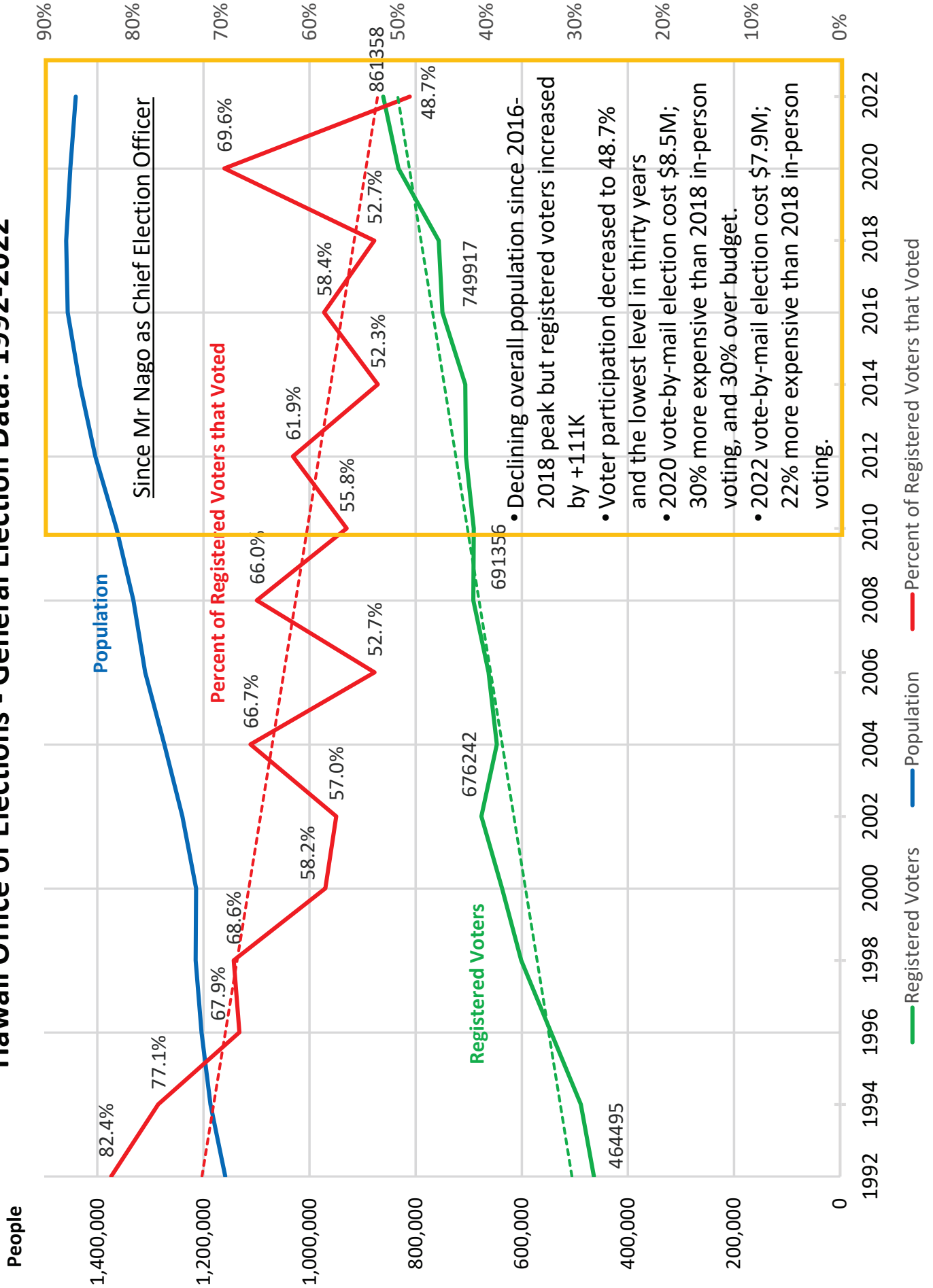
Joining ERIC would provide another tool for election officials to maintain the accuracy and integrity of the voter registration rolls by allowing us to compare our voter registration file and driver license/identification card file with other member states. This will permit election officials to determine if a voter has moved out of state, as they register to vote or obtain a driver license in another jurisdiction. Additionally, ERIC membership requires all driver license/identification card holders who are eligible to register to vote, but are not currently registered, to be sent a mailer encouraging them to register.

Since our previous testimony on measures related to joining ERIC, we have received updated information on costs. We estimate that it will cost \$149,000 in FY 2024-25 to join ERIC based on the \$25,000 application fee, \$42,500 annual membership fee, and approximately \$81,500 to conduct the initial mailing to driver license and state identification card holders who are not

registered to vote as required for membership in ERIC, along with mailings to address in-state movers and cross-state movers. The recurring costs, which we would submit as part of our annual budget request starting with FY 2025-26, would be approximately \$45,000 for the annual membership fee, which is recalculated each year by ERIC.

Thank you for the opportunity to testify in support of Senate Bill No. 2240,
SD 2.

Hawaii Office of Elections - General Election Data: 1992-2022



From: [Loree Searcy](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Reinstating Nago supplemental testimony
Date: Monday, March 18, 2024 11:57:13 AM

I am opposed to reinstating Mr. Nago as Chief Elections Officer because while he did hold this office he had a poor performance history not being truthful and responsible to The People for election integrity!

He is not a person I want to see in a position of authority!

Loree Searcy

Mahalo

Sent from my iPhone

TESTIMONY

Hawaii Elections Commission

Tuesday, March 19, 2024, 1:30 p.m., Via Videoconference

Chair Curtis and Commission Members:

My name is Janet Mason. I am a retired business executive and live in Honolulu. I have worked as an Elections Observer for both primary and general elections since at least 2016. My work as an Observer has usually been at the State Counting Center on Oahu, but several times I have also observed the ballot processing operations at the City and County of Honolulu. I am also certified as a Short-Term Observer by the United Nations Office for Democratic Institutions and Human Rights.

Discussion of the Evaluation and Reappointment of the Chief Elections Officer

Evaluation of the performance of the Chief Election Officer is a statutory duty of this Commission. Hawaii is fortunate to have a bipartisan Elections Commission; this helps keep the conduct of our elections independent from partisan politics (a basic democratic principle). Your January and February meetings were difficult, but I congratulate Chair Curtis for managing these meetings fairly.

I accept that all of you are making a good faith effort to conduct a professional, thorough evaluation of Mr. Nago's performance. I defer to your decision about this. But to complete this work I assume you are interested in the perspective of volunteer Election Observers like me because we are the "eyes and ears of the public" during election operations.

Based on my experience over the past eight years, I am happy to tell you I have no reservations about Hawaii's elections processing. For example, I have never seen a ballot under the exclusive control of one person. I have never seen mobile phones in use at the Counting Center. Because I have participated in pre-election testing of "live" ballots and post-election testing after all real ballots have been reported on election day, I am confident that our ballot scanners work; they correctly scan ballots, and the associated software correctly tabulates the results of voted ballots. All such procedures have been carefully maintained and documented under Mr. Nago's leadership, and all procedures are the same statewide. Hawaii's voters should have strong confidence that they can register to vote, then vote in a convenient and secure way.

Together the Counties and the State have been immensely successful in improving the number of eligible citizens who have registered to vote, especially since the introduction of automatic voter registration in 2021. Mr. Nago actively supported this change because he understood it would increase access to registration and help improve the accuracy of voter rolls by sharing data between the driver's license database, state ID database and the statewide voter registration system.

Does this mean errors never occur and our elections are flawless? It does not. Each election presents an opportunity for process improvements. For example, automatic recounts of close state elections were not conducted in Hawaii until 2020. Since then, the Office of Elections conducted 11 automatic recounts, most resulting from small single-party primaries. During the 2022 primary when the legal threshold for close elections was equal to 100 votes or .25 percent of the votes cast,

(whichever was **greater**) the Office of Elections incorrectly conducted a recount for the District 20 representative seat. Here the vote difference was 87, and the percentage difference was 6.7 percent. It wasn't until 2024, when Mr. Nago testified at the Legislature, that the language for the mandatory threshold for recounts was corrected to be equal to 100 votes or .25 percent, whichever is **lesser**.

In conclusion, I have seen firsthand steady process improvements in our elections administration over the past decade.

Thank you for the opportunity to present my testimony.

From: [Lorraine Larzabal](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Chief Election Officer Tues March 19th
Date: Monday, March 18, 2024 12:42:38 PM

I oppose reinstating Scott Nago.
He introduced legislation to eliminate ballot audits.
HRS 11-7.5(6) states the public's right of review. There has not been a public review of his performance in years. Why?

Lorraine Larzabal
Lihue, HI

From: [Robert Hastings](#)
To: [OE.Elections](#)
Cc: [Keli'i Akina](#); [Joe Kent](#)
Subject: [EXTERNAL] Cleaning voter rolls
Date: Monday, March 18, 2024 2:46:00 PM

Elections Commission:

When I registered to vote in Hawaii over 45 years ago, I was told by the Registrar that it was important that I vote, as the law would require my registration to be cancelled if I failed to vote in two consecutive election cycles. That law has not been enforced in Hawaii for many years, as I am aware of individuals who moved away many years ago who are still on the rolls and were sent mail-in ballots despite not having voted in Hawaii or returned the yellow confirmation cards that were sent to their old addresses. I've read of others who are aware of this as well.

The rolls need to be purged as required by law, both to ensure election integrity and more accurately report the percentage of voters who vote.

Please address this issue.

Aloha,
Robert Hastings

Hastings Laun & Houser LLLC
65-1230 Mamalahoa Hwy., Ste. B20
Kamuela, HI 96743
[\(808\) 885-4554](tel:8088854554)

From: Shkpah7@protonmail.com
To: [OE.Elections](#)
Subject: [EXTERNAL] Elections Commission Mtg on 3/19/24 Written Testimony
Date: Monday, March 18, 2024 3:06:38 PM

Aloha Elections Commission,

Please do not reappoint Scott Nago as Chief Election Officer (or to any other position)!

Hawaii has the lowest voter confidence in elections of any state in the country.

Instead of an eagerness or even willingness to demonstrate why our system can be trusted, Scott Nago has put ten times as much energy into opaqueness, making up his own rules, and backing bills that make it even more difficult to audit the vote, and to prove the reliability of our system.

I urge you to look for and appoint someone with the exact opposite mindset of Mr Nago!

Such a change would be welcomed, beneficial, and supported by the citizens of the state of Hawaii.

Sincerely,

Scott Shedko

Sent with [Proton Mail](#) secure email.

From: [Steve B](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Scott Nago
Date: Monday, March 18, 2024 3:12:56 PM

Anybody but Scott Nago for Chief Election Officer!

From: [Jade Brown](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] re-appointment of Scott Nago
Date: Monday, March 18, 2024 3:45:26 PM

This communication is intended for the NOTICE OF ELECTIONS COMMISSION MEETING occurring Tuesday, March 19th at 1:30 p.m

I do not support the re-appointment of Scott Nago because he demonstrates that he is willing to compromise election integrity. Perhaps the most glaring example of this occurred in the HI 2020 election. Chain of custody of ballots was not protected. This is a known fact and is available on the record in public testimony. Maintaining chain of custody of election ballots is not complicated and procedures could have been implemented and carried out. The HI CEO must surely meet this most basic minimum standard. Saying it was an unfortunate result of the pandemic/mail-in ballots and promises to do better next time are insufficient because there is no available remedy to fix the harm that was done to the HI 2020 election. Please protect the integrity of HI elections.

Jade L Brown

From: [Halina Ngo](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] NAGO
Date: Monday, March 18, 2024 4:22:32 PM

We are opposing he reelection. Terrible leadership while in office.
Thank you!

From: [Peter Baldwin](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Election Commission and Election of Scott Nago
Date: Monday, March 18, 2024 4:34:49 PM

Dear Members of the Election Commission:

In my opinion election integrity is the most fundamental issue we face in the State of Hawaii. Many of us, including myself, no longer feel the elections are fair, and feel the reliance on machines rather than humans to run elections and count the votes is causing voter distrust of the system. Mail in votes, drop boxes and the lack of voter IDs are all leading us down the path of dishonest elections and I hope and pray we can return to an election day, human run election until we can work all the bugs out of the current system.

In my review of Scott Nago, I believe our Hawaii voters would be better served if he were not re-elected. Someone new needs to be sought and elected to fill this position in order to begin to re-establish trust in our elections.

Thank you.

Peter Baldwin
Koloa, Kauai

From: [Terri Yoshinaga](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Request a public hearing to oppose the appointment of Scott Nago!
Date: Monday, March 18, 2024 5:40:44 PM

The Governor, legislators, and the election commission must be fair and take into account the people's testimonies. I listened to oral testimony last time which are valid issues to remove Scott Nago. Please do the right thing for the people of Hawaii!

Sent from my iPhone

From: [Cindy Pang](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Written Testimony Chief
Date: Monday, March 18, 2024 6:00:01 PM

Re: ELECTIONS COMMISSION MEETING Tues, 3/19 at 1:30 PM

Request: Do NOT reappoint Scott Nago as Chief Election Officer. His performance has been very ineffective — voter turnout has decreased & litigation increased under his watch.

Thank you.

From: [Jacqueline Nakamura](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Votes
Date: Monday, March 18, 2024 6:13:14 PM

Aloha

As a citizen on the USA I have never not voted in an election in person until I moved here to hawaii.

It was also very difficult to turn in a ballot to a person I am not comfortable putting my right to vote in a box in front of a building and not feeling comfortable of what is going to happen to my vote. We need integrity back in our elections and we need to clean up the voter rolls! Should not take a lawsuit to do the right thing.

Mahalo
Jackie Nakamura
Sent from my iPhone

From: [Mike Nakamura](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Voter integrity
Date: Monday, March 18, 2024 6:57:25 PM

To Election Commission Chair

Our Hawaii elections are not transparent, nor trustworthy.

Hawaii has:

Declining voter participation.

Lowest voter turnout on record.

Inflated voter rolls (up 110K since 2016 but with lower participation...)

More than 20 court cases filed

in 2023 challenging application of statutory laws.

Continued disregard for Election Commission

Enough. Who would not want fully transparent and legal elections? Does anyone have an answer for this?

Why in 2020 did it take so long to get a vote count?

Weak elections favor weak governments.

Thank you.

Mike Nakamura

Sent from my iPhone

From: [Melissa A. Aiona](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] DO NOT RE Elect Scott Nago for chief elections officer
Date: Monday, March 18, 2024 8:37:52 PM

I want to make my voice heard and my opinion recorded... I DO NOT think Scott Nago deserves to be appointed to chief elections officer.... He has not proven to be of solid character... and needs to be removed. Hawaii needs to clean house... and remove these irresponsible people... replace them with people who actually care about the future of Hawaii.
Thank you
Melissa Aiona

From: [Alika Aloha](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Chief Election Officer
Date: Tuesday, March 19, 2024 1:48:38 AM

I am writing to voice my opposition to Scott Nago being reelected as Chief Elections Officer. He has a dismal track record with inflated voters rolls and the lowest votes turnout in Hawaii's history.

It's time for new, honest leadership.

Vote no.

Alice Abellanida
Waianae

From: [JO ANN OCHI](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Scott Nago
Date: Tuesday, March 19, 2024 2:24:21 AM

To the committee,

Regarding Scott Nago I am expressing my opinion that the rules should be followed and reappointment should be invalid. If a person is not doing anything to benefit the people of Hawaii, but just himself then he has no business holding office. That's a majority of most of you in office!!

Jo Ann Ochi
Sent from my iPhone

From: [JO ANN OCHI](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Scott Nago
Date: Tuesday, March 19, 2024 2:24:21 AM

To the committee,

Regarding Scott Nago I am expressing my opinion that the rules should be followed and reappointment should be invalid. If a person is not doing anything to benefit the people of Hawaii, but just himself then he has no business holding office. That's a majority of most of you in office!!

Jo Ann Ochi
Sent from my iPhone

From: [Joe Pacheco](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Elections Commission Meeting ID: 820 3104 1040 (3/19/2024 - 1:30pm)
Date: Tuesday, March 19, 2024 5:04:14 AM

Written testimony for the:
Elections Commission Meeting ID: 820 3104 1040 (3/19/2024 - 1:30pm)

Aloha,

I am writing to express my disappointment in the way elections are being run under the current administration and how it is time for change.

Election integrity is at an all-time low across this country, and Hawai'i/Honolulu is no different.

Too many citizens question the current election process, which in turn causes; the all time low trust in the system, and the questioning of the integrity and easily manipulated process of mail-in voting, with its lack of identification or in person identification of individuals participating in our most sacred of citizen actions. Covid was used as an excuse to instigate some of these changes (but now we know better), and those changes are still in place even though they are no longer needed. i.e. mail-in voting, lack of identification.

As a voting citizen of 61 years of age, before the use of computers and tabulators, we knew election results before we went to bed that evening. Now it takes days, if not longer (some states months), for us to get results, opening up the suspicion, or actual use of, election fraud practices.

It is time for change (regardless of party affiliation) for fairness, integrity, accuracy, and good old-fashioned trust in the United States election process, and in turn, the U.S. government itself.

If Hawai'i State elections are your *kuleana*, it is time for you to step aside for change and improvement.

If it is your *kuleana* to evaluate and appoint individuals in charge of Hawai'i's elections, it is time for you to MAKE a change.

Sincerely & Mahalo,
Joe Pacheco
U.S. Citizen and Hawaii Resident

From: [Alex Akui](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Scott Nago
Date: Tuesday, March 19, 2024 5:25:17 AM

You should NOT vote to reappoint Scott Nago as Hawaii Chief Election Officer!
[Yahoo Mail: Search, Organize, Conquer](#)

From: [James](#)
To: [OE.Elections](#)
Subject: [EXTERNAL]
Date: Tuesday, March 19, 2024 5:40:38 AM

Please do not reappoint Scott Nago as a Chief Election Officer. He is a big time failure the last 3 elections or more and is getting worst. Get rid of this rigger.

From: [Vivek Pathela](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] OOPPOSE Re-Election of Scott Nago
Date: Tuesday, March 19, 2024 6:48:34 AM

Dear Commissioners:

I humbly OPPOSE the re-election of Scott Nago. Election Integrity is now recognized to be one of the worst in Hawaii. The People of Hawaii have lost confidence in our Elections, and we have the lowest voter turnout. There are inflated voter rolls with over 100,000 inactive. It's imperative Hawaii has a fresh, fair and competent Chief Elections Officer that serves the People of Hawaii.

The following are issues uncovered while Scott Nago is in charge:

- Mailing errors in the thousands
- Signature verification issues
- Unexplained mismatched official data releases
- Early deployment of ballot boxes that were left completely unmonitored
- Failure to register voters through the DMV process
- Voter rolls that are admittedly filled with up to 100 k deadwood voters and proof of ballots being sent to properties for voters that do not reside there
- Computer voting systems that are not fully secured and tested & a lack of knowledge in managing technology & technology vendors
- Cast Vote Record data not being available or usable
- Data showing that Joe Biden received more votes in the 2020 presidential election than Barack Obama in his home state
- Secrecy of the ballot not being ensured for in-person voting
- US Code election record retention requirements not being met
- As well as Hawaii statutory rules regarding audits and chain of custody being broken

I oppose Scott Nago's re-election.

Kind regards,
Vivek

Vivek Pathela
5231 Kuaiwi Pl
Honolulu, HI 96821

408-772-6388
vpathela@gmail.com

From: [Lorraine Nip](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Reappointment of Scott Nago
Date: Tuesday, March 19, 2024 7:17:42 AM

Rules should be followed and the reappointment of Scott Nago as C.E.O. should be invalid!

Hawaii needs to rebuild trust in our election system. We need an audit after each election and full transparency.

Sent from my iPhone

From: [Kayla Kawamura](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Testimony
Date: Tuesday, March 19, 2024 7:27:44 AM

Aloha,

In a free country like America, its citizens' freedoms and rights should be protected at all costs. This includes the impact of each individual's vote! The people of Hawaii should have every ounce of confidence that their election process is secure. Voter turnout will continue to decline if the people of Hawaii believe their elections are not fair or secured. The Chief Election Officer should listen to the people of Hawaii's concerns and uphold the integrity of the election process to the highest degree. The high volume of court cases filed in 2023 challenging the application of statutory laws is rather alarming. As we prepare for an upcoming election in November, I will fully support the reappointment of a new Chief Election Officer who will maintain transparency and restore faith in the election process for all the people of Hawaii.

Thank you,
Kayla Kawamura

From: [Mark Masunaga](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Oppose re-election of Scott Nago
Date: Tuesday, March 19, 2024 8:08:26 AM

I oppose re-election of Scott Nago. Despite denials , the election system has lost integrity. Covid is now over and elections should return to vote in person . Mail in voting has been a failure of election integrity with errors in the thousands. These are some of the issues while Scott Nago was in charge.

Mailing errors in the thousands

Signature verification issues

Ballot boxes not monitored, I saw this myself
chain of custody broken

In short Scott Nago has been either incompetent, corrupted , or both in his duties. He works for the

citizens . We do not want him re-elected .

Mark Masunaga

From: [David Hawaii](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Testimony -Pursuant to Section 3-170-11,
Date: Tuesday, March 19, 2024 8:15:13 AM

Aloha,

I am writing to express my strong opposition to the reappointment of Scott Nago for the position of Hawaii Elections Officer. Despite his tenure, Mr. Nago has failed to uphold the fundamental principles of fair and accessible elections, and his continued presence in this role would only serve to further undermine our democratic process.

One of the most glaring failures of Mr. Nago's leadership is the consistently low voter turnout in Hawaii under his watch. The right to vote is a cornerstone of our democracy, yet Hawaii consistently ranks among the lowest in voter participation rates nationwide. This dismal turnout reflects a systemic failure to engage and empower voters, and Mr. Nago must be held accountable for this unacceptable state of affairs.

Furthermore, Mr. Nago has demonstrated a blatant disregard for the recommendations and directives of the Elections Commission, further eroding public trust in the integrity of our electoral system. The commission exists to ensure that elections are conducted fairly and transparently, yet Mr. Nago has repeatedly ignored their guidance, choosing instead to operate with impunity.

Additionally, Mr. Nago's tenure has been marred by more than 20 court cases filed against him, raising serious concerns about his ability to effectively lead the Hawaii Elections Office. These legal challenges point to a pattern of incompetence and negligence that simply cannot be tolerated in such a critical role. This does not necessarily mean he is guilty of anything, though focusing on the facts of our voter turnout is my larger oversight idea.

In light of these significant shortcomings, it is clear that Mr. Nago is not fit to continue serving as Hawaii Elections Officer. We need a leader who is committed to fostering a culture of civic engagement and ensuring that every eligible voter has the opportunity to participate in our democratic process. The reappointment of Mr. Nago would only perpetuate the status quo of disenfranchisement and dysfunction, and I urge you to consider the best interests of the people of Hawaii by seeking a new candidate for this vital position.

David Silva

Lifetime Hawaii resident

From: [chester lum](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Written Testimony for Elections Commission Meeting on Tuesday March 19, 2024 at 1:30PM
Date: Tuesday, March 19, 2024 8:27:25 AM

Thank you for allowing me to submit written testimony opposing the reappointment of Scott Nago as the Chief Election Officer.

The current Chief Election Officer has not followed the law in doing ten per cent of the precincts employing the electronic voting system, to verify that the electronic tallies generated by the system for all elections in those precincts equal hand tallies of the paper ballots generated by the system for all elections in those precincts for the past election cycles.

Our votes are sacred and as a paid Chief Executive Officer of taxpayer's money, it is his responsibility to ensure that the will of the people is accurately represented. To date, he has FAILED.

Once again, thank you for allowing me to submit written testimony opposing the reappointment of Scott Nago as the Chief Election Officer.

Chester Lum

From: [Selina L](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Re-election of Chief Elections Officer Opposition
Date: Tuesday, March 19, 2024 8:32:43 AM

Aloha mai Kaua,

I oppose the re-election of Scott Nago as chief elections officer. Everything in the dark is coming to the light and Scott Nago is not a man of integrity or righteousness that should have any power in Hawai'i.

Mahalo,
K Selina Lalau-Hitchcock

March 16, 2024

Elections Commission
c/o Office of Elections
802 Lehua Avenue
Pearl City, HI 96782

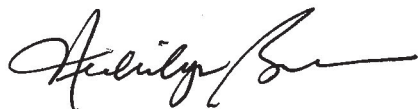
Dear Chair Curtis and Members of the Commission,

I am writing to express my strong support of the reappointment of Scott Nago as Chief Election Officer.

I have been with the Office of Elections for 10 years under the direction of Mr. Nago. Mr. Nago's commitment to the work of elections is unmatched because of the experience he brings to the job. Mr. Nago understands elections inside and out. He understands and respects the laws that govern our elections but also understands that the times and elections evolve which is why he continuously seeks to improve the process. I have witnessed him take on challenges head-on from having to deal with natural disasters and most notably conducting elections during the pandemic. Election work is not easy, but Mr. Nago is dedicated to the job and and to the mission of the Office of Elections.

Thank you for the opportunity to provide testimony in support of Scott Nago's reappointment of Chief Election Officer.

Best Regards,

A handwritten signature in black ink, appearing to read "Nedielyn Bueno", with a long horizontal flourish extending to the right.

Nedielyn Bueno

From: [Joy Dillon](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Oppose Reappointment of Scott Nago
Date: Tuesday, March 19, 2024 12:54:36 PM

Hello, Elections Committee.

I strongly oppose the reappointment of Scott Nago as Chief Elections Officer. Under his watch we have had the lowest voter turnout in history and inflated voter rolls that need to be cleaned up. He has had more than 20 court cases filed against him but still he keeps his job! Why? Scott Nago has shown continued disregard for the Elections Commission. I urge you not to reappoint him and work toward safe and secure voting. Thank you for your consideration

Joy Dillon
Hilo Resident
808-640-2544 Cell
joy@joydillon.com

From: [Barilyne Sakamoto](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Do NOT reappoint Scott Nago as the Chief Election Officer
Date: Tuesday, March 19, 2024 1:12:32 PM

Aloha,

Do NOT reappoint Scott Nago as Chief Election Officer. His performance has been very ineffective, voter turnout has decreased & litigation increased under his watch. Please appoint someone who will bring integrity and effectiveness in this position.

Warmest regards,

Barilyne Sakamoto - Concern citizen
3911-A Keanu Street
Honolulu, HI 96816

From: [David Williams](#)
To: [OE.Elections](#)
Subject: [EXTERNAL] Please do not reelect Scott Nago
Date: Tuesday, March 19, 2024 1:47:45 PM

Strongly oppose the reelection of Scott Nago

Too many inconsistencies, with the way, he's running things, voter turnout is that an all time low, trust in the voting system all time low and he's doing nothing to gain the Trust of the people. He is not being transparent with the way the elections are being run.. in my eyes he is incredibly untrustworthy, and should not be reelected.

Sent from my iPhone

From: [Adriel Lam](#)
To: [OE.Elections](#)
Cc: county.clerk@mauicounty.us; elections@honolulu.gov; elections@kauai.gov; hiloelec@hawaiicounty.gov
Subject: [EXTERNAL] Election Commission Meeting 3/19/24
Date: Tuesday, March 19, 2024 2:09:06 PM
Attachments: [23- PetitionForWritOfCertiorari.pdf](#)
[unclearballot.pdf](#)

Aloha, please provide the attached documents for the Election Commissioners for review.

Pg 13 of Unclear Ballot

We also collected timing data while processing Clackamas County ballots. Running on a system with a 4-core Intel E3-1230 CPU running at 3.40 GHz with 64 GB of RAM, UnclearBallot took an average of 279 ms to process each ballot. For reference, Hart's fastest central scanner's maximum scan rate is one ballot per 352 ms [37], well above the time needed to carry out our attack.

Pg 27 of Petition for Writ of Certiorari

Dominion configured its machines with the decryption keys in an election database table in plain text—protected by nothing other than Windows log-in credentials that are easily bypassed—enabling any malicious actor total control over its electronic voting systems. This security breach violates *common sense*, to say nothing of FIPS-level encryption.

Aloha,
Adriel

No. __-____

In the Supreme Court of the United States

KARI LAKE AND MARK FINCHEM,
Petitioners,

v.

ADRIAN FONTES,
ARIZONA SECRETARY OF STATE, *ET AL.*,
Respondents.

ON PETITION FOR WRIT OF *CERTIORARI*
TO THE U.S. COURT OF APPEALS
FOR THE NINTH CIRCUIT

PETITION FOR WRIT OF *CERTIORARI*

KURT B. OLSEN
Olsen Law PC
1250 Connecticut Ave. NW
Suite 700
Washington, DC 20036
202-408-7025
ko@olsenlawpc.com

LAWRENCE J. JOSEPH
Counsel of Record
1250 Connecticut Ave. NW
Suite 700
Washington, DC 20036
202-355-9452
ljoseph@larryjoseph.com
Counsel for Petitioners

QUESTIONS PRESENTED

As 2022 candidates for Governor and Secretary of State, petitioners sued Arizona’s Secretary of State and two counties to challenge whether electronic voting machines assure a fair and accurate vote under the Due Process Clause and their rights as candidates and voters. Petitioners also sought a preliminary injunction, and six cyber or national-security experts testified on the voting machines’ unsuitability to provide a secure and accurate vote. The testimony and evidence showed actual electronic vote tampering in prior elections, which the district court disregarded in finding petitioners’ claims too speculative for Article III standing, based in part on safeguards the counties claimed to follow. The Ninth Circuit affirmed citing, *inter alia*, *Lance v. Coffman*, 549 U.S. 437 (2007), for the lack of particularized injury in voters’ challenges. New evidence from other litigation and public-record requests shows defendants made false statements to the district court regarding the safeguards allegedly followed to ensure the accuracy of the vote, on which the district court relied. That enables petitioners to seek to amend their allegations on standing under 28 U.S.C. §1653 to show a non-speculative likelihood that the same harms will recur in future elections, which harms did indeed occur in the 2022 election.

The questions presented are:

1. Whether an Article III case or controversy existed at all relevant times and still exists.
2. Whether petitioners may amend their allegations of jurisdiction under §1653 to allege recently discovered pre-litigation injury.
3. Whether petitioners’ injuries—if moot—are nonetheless capable of repetition, yet evading review.

PARTIES TO THE PROCEEDING

Petitioners are Kari Lake and Mark Finchem, who were plaintiffs in District Court and appellants in the Court of Appeals.

Respondents are Adrian Fontes in his official capacity as Arizona Secretary of State, the Maricopa County Board of Supervisors, Bill Gates, Clint Hickman, Jack Sellers, Thomas Galvin, and Steve Gallardo in their official capacities as members of the Maricopa County Board of Supervisors, and Rex Scott, Matt Heinz, Sharon Bronson, Steve Christy, and Adelita Grijalva in their official capacities as members of the Pima County Board of Supervisors, who were defendants in District Court and appellees in the Court of Appeals. (Secretary Fontes substituted for his predecessor pursuant to FED. R. APP. P. 43(c)(2).)

RULE 29.6 STATEMENT

Petitioners are natural persons with no parent companies and no outstanding stock.

STATEMENT OF RELATED CASES

This case arises from and is related to the following proceedings in the U.S. District Court for the District of Arizona and the U.S. Court of Appeals for the Ninth Circuit under S.Ct. Rule 14.1(b)(iii):

- *Lake v. Hobbs*, No. 2:22-cv-0677-JJT (D. Ariz. decided Aug. 26, 2022).
- *Lake v. Fontes*, No. 22-16413 (9th Cir. decided Oct. 16, 2023).
- *Lake v. Fontes*, Nos. 23-16022, 23-16023 (9th Cir. docketed Jul. 24, 2023).

Although other cases challenged respondents' actions in the 2022 election, no other case relates to this case within the meaning of Rule 14.1(b)(iii).

TABLE OF CONTENTS

Questions Presented	i
Parties to the Proceeding	ii
Rule 29.6 Statement.....	ii
Statement of Related Cases	ii
Appendix.....	vi
Table of Authorities.....	vii
Petition for Writ of <i>Certiorari</i>	1
Opinions Below.....	1
Jurisdiction.....	1
Statutory Provisions Involved	1
Statement of the Case	1
I. Legal Background	4
A. Standing under Article III	4
B. Sovereign Immunity and <i>Ex parte Young</i>	5
C. Amended Jurisdictional Allegations under 28 U.S.C. §1653.....	5
II. Factual Background.....	6
A. The record before the district court.	7
1. The complaint’s allegations.	7
2. The preliminary injunction evidence.	9
B. Maricopa’s chaotic 2022 election.....	11
C. New evidence of misconduct in prior elections.	11
III. Procedural Background	13
Reasons to Grant the Writ.....	14
I. The district court had and still has jurisdiction to resolve this action.	14
A. Petitioners had and still have Article III standing.	15

1. Petitioners suffer particularized and concrete injury from Maricopa’s unlawful election practices.	16
a. This Court can consider new allegations related to standing.	17
b. Petitioners’ injuries are actual and imminent, not speculative.....	19
c. Petitioners’ injuries are concrete and particularized, not abstract or generalized.	21
(1) Candidates and political parties suffer injury.	22
(2) Voters suffer injury.	23
2. Petitioners’ procedural injuries lower the Article III threshold for immediacy and redressability.	24
3. Past injuries are evidence of future injury.	24
4. Petitioners’ injuries are traceable to Maricopa’s and the Secretary’s actions and redressable in court.....	25
5. Petitioners’ standing covers any way that Maricopa violated election law.	26
a. Article III has no nexus requirement outside the Establishment Clause.	26
b. This Court should narrow <i>Lance</i> to its holding for voter standing under the Elections Clause.	27
B. This action was and remains ripe.....	28
C. This action is not moot.	29

1.	As voters and future candidates, petitioners still suffer injury redressable in future elections.	29
2.	Even a complaint directed against only the 2022 election could avoid mootness as capable of repetition yet evading review.	29
D.	There is no “ <i>Purcell</i> problem” for <i>future</i> elections.	30
E.	Sovereign immunity poses no barrier.....	31
1.	The county respondents lack sovereign immunity.	31
2.	Sovereign immunity does not protect ongoing violations of federal law.	32
a.	State election law is enforceable under the Elections Clause.	32
b.	State election law is enforceable under §1988(a).	33
c.	State election law informs what “process” is “due” regarding the fundamental right to vote.	33
II.	This Court should summarily reverse, both on the original record and <i>a fortiori</i> on the new evidence under §1653.....	34
A.	It is urgent to resolve these issues before the 2024 election.....	35
B.	The district-court record supports summary reversal.....	35
C.	New allegations under §1653 <i>a fortiori</i> support summary reversal.....	36
III.	The questions presented are crucial to ensuring electoral integrity.	36

A. The fundamental right to vote is
“preservative of all rights,” and only this
Court can secure that right..... 37

B. The Court should commit to taking up
cases alleging electoral improprieties..... 37

Conclusion 38

APPENDIX

Lake v. Fontes, No. 22-16413 (9th Cir. Oct. 16,
2023) 1a

Lake v. Hobbs, No. 2:22-cv-0677-JJT (D. Ariz.
Aug. 26, 2022) 10a

U.S. CONST. art. I, § 4..... 40a

U.S. CONST. art. II, § 1, cl. 2 40a

U.S. CONST. amend. XI..... 40a

U.S. CONST. amend. XIV, §1 40a

28 U.S.C. §1653 40a

42 U.S.C. §1988(a)..... 41a

A.R.S. §16-442 41a

A.R.S. §16-449 44a

A.R.S. §16-452 45a

A.R.S. §16-1004 46a

A.R.S. §16-1009 47a

A.R.S. §16-1010 47a

Amended Compl. (May 4, 2022)..... 48a

Declaration of Walter C. Daugherty (June 8,
2022) 113a

Declaration of Benjamin R. Cotton (June 8,
2022) 130a

Hearing Transcript (July 21, 2022) (excerpt)..... 144a

TABLE OF AUTHORITIES**Cases**

<i>Alden v. Maine</i> , 527 U.S. 706 (1999).....	31
<i>Ariz. State Legis. v. Ariz. Indep. Redistricting Comm'n</i> , 576 U.S. 787 (2015)	35
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007).....	25
<i>Bennett v. Spear</i> , 520 U.S. 154 (1997).....	5
<i>Bognet v. Degraffenreid</i> , 141 S.Ct. 2508 (2021).....	28
<i>Bognet v. Sec’y Pa.</i> , 980 F.3d 336 (3d Cir. 2020)	28
<i>Bonas v. Town of N. Smithfield</i> , 265 F.3d 69 (1st Cir. 2001)	23
<i>Campbell-Ewald Co. v. Gomez</i> , 577 U.S. 153 (2016).....	29
<i>Carney v. Adams</i> , 141 S.Ct. 493 (2020).....	4
<i>Carson v. Simon</i> , 978 F.3d 1051 (8th Cir. 2020).....	22, 28
<i>City of Waukesha v. EPA</i> , 320 F.3d 228 (D.C. Cir. 2003)	35
<i>Cleveland Bd. of Educ. v. Loudermill</i> , 470 U.S. 532 (1985).....	33
<i>Clinton v. City of New York</i> , 524 U.S. 417 (1998).....	22
<i>Crawford v. Marion County Election Bd.</i> , 553 U.S. 181 (2008).....	22

<i>Curling v. Raffensperger</i> , __ F.Supp.3d __, 2023 U.S. Dist. LEXIS 202368 (N.D. Ga. Nov. 10, 2023)	3, 20
<i>Curling v. Raffensperger</i> , 494 F.Supp3d 1264 (N.D. Ga. 2020).....	3
<i>DaimlerChrysler Corp. v. Cuno</i> , 547 U.S. 332 (2006)	26-27
<i>Diffenderfer v. Cent. Baptist Church, Inc.</i> , 404 U.S. 412 (1972)	30
<i>Dittman v. California</i> , 191 F.3d 1020 (9th Cir. 1999)	15
<i>Donald J. Trump for President, Inc. v. Sec’y Pa.</i> , 830 F.App’x 377 (3d Cir. 2020)	28
<i>Duke Power Co. v. Carolina Envtl. Study Grp.</i> , 438 U.S. 59 (1978)	26-27
<i>Edelman v. Jordan</i> , 415 U.S. 651 (1974)	31
<i>Ex parte Young</i> , 209 U.S. 123 (1908)	31-32
<i>FEC v. Akins</i> , 524 U.S. 11 (1998)	21-22, 24
<i>FEC v. Wisconsin Right to Life, Inc.</i> , 551 U.S. 449 (2007)	30
<i>Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.</i> <i>(TOC), Inc.</i> , 528 U.S. 167 (2000)	29-30
<i>Fulani v. League of Women Voters Educ. Fund</i> , 882 F.2d 621 (2d Cir. 1989)	22
<i>Garcia v. Sedillo</i> , 70 Ariz. 192 (1950)	18
<i>Gill v. Whitford</i> , 138 S.Ct. 1916 (2018)	21

<i>Golonka v. GMC</i> , 204 Ariz. 575 (App. 2003)	19
<i>Hunt v. Campbell</i> , 19 Ariz. 254 (1917)	18
<i>In re Lake</i> , No. 23A622 (2024)	1
<i>Kingdomware Techs., Inc. v. United States</i> , 579 U.S. 162 (2016)	29
<i>Krislov v. Rednour</i> , 226 F.3d 851 (7th Cir. 2000)	16, 23
<i>Lake v. Fontes</i> , 83 F.4th 1199 (9th Cir. 2023)	1
<i>Lake v. Hobbs</i> , 623 F.Supp.3d 1015 (D. Ariz. 2022)	1
<i>Lambrix v. Singletary</i> , 520 U.S. 518 (1997)	34
<i>Lance v. Coffman</i> , 549 U.S. 437 (2007)	2-4, 14, 24, 26-28, 34-35
<i>Lawrence v. Chater</i> , 516 U.S. 163 (1996)	34
<i>Lewert v. P.F. Chang's China Bistro, Inc.</i> , 819 F.3d 963 (7th Cir. 2016)	20, 25
<i>Lewis v. Casey</i> , 518 U.S. 343 (1996)	27
<i>Lujan v. Defenders of Wildlife</i> , 504 U.S. 555 (1992)	4-5, 24-25
<i>Lynch v. Household Fin. Corp.</i> , 405 U.S. 538 (1972)	33
<i>Massachusetts v. EPA</i> , 549 U.S. 497 (2007)	26, 38
<i>Mecinas v. Hobbs</i> , 30 F.4th 890 (9th Cir. 2022)	16, 22

<i>Moor v. County of Alameda</i> , 411 U.S. 693 (1973)	33
<i>Moore v. Harper</i> , 143 S.Ct. 2065 (2023)	4, 14, 32, 34
<i>Nader v. Blackwell</i> , 545 F.3d 459 (6th Cir. 2008)	23
<i>Newman-Green, Inc. v. Alfonzo-Larrain</i> , 490 U.S. 826 (1989)	5-6
<i>Northeastern Fla. Chapter of Associated Gen. Contractors of Am. v. City of Jacksonville</i> , 508 U.S. 656 (1993)	19
<i>Northern Ins. Co. v. Chatham Cty.</i> , 547 U.S. 189 (2006)	31-32
<i>O'Shea v. Littleton</i> , 414 U.S. 488 (1974)	25
<i>Ohio Forestry Ass'n v. Sierra Club</i> , 523 U.S. 726 (1998)	28
<i>Oregon v. Mitchell</i> , 400 U.S. 112 (1970)	37
<i>Pedersen v. Bennett</i> , 230 Ariz. 556 (2012)	11
<i>Pennhurst State Sch. & Hosp. v. Halderman</i> , 465 U.S. 89, 106 (1984)	32-33
<i>Perez v. Ledesma</i> , 401 U.S. 82 (1971)	31
<i>Purcell v. Gonzalez</i> , 549 U.S. 1 (2006)	1, 13, 15-16, 22, 30-31
<i>Regents of the Univ. of California v. Bakke</i> , 438 U.S. 265 (1978)	19
<i>Reynolds v. Sims</i> , 377 U.S. 533 (1964)	20, 23

<i>Rose v. Mitchell</i> , 443 U.S. 545 (1979).....	38
<i>Ruhrigas Ag v. Marathon Oil Co.</i> , 526 U.S. 574 (1999).....	15
<i>Shaw v. Reno</i> , 509 U.S. 630 (1993).....	23
<i>Shays v. FEC</i> , 414 F.3d 76 (D.C. Cir. 2005).....	22-23
<i>Silva v. Traver</i> , 63 Ariz. 364 (1945).....	19
<i>Singleton v. Wulff</i> , 428 U.S. 106 (1976).....	15
<i>Sochor v. Florida</i> , 504 U.S. 527 (1992).....	6
<i>Spokeo, Inc. v. Robins</i> , 578 U.S. 330 (2016).....	21
<i>Spomer v. Littleton</i> , 414 U.S. 514 (1974).....	30
<i>State v. Arevalo</i> , 249 Ariz. 370 (2020).....	34
<i>Stewart v. Blackwell</i> , 444 F.3d 843 (6th Cir. 2006).....	16, 23
<i>Summers v. Earth Island Inst.</i> , 555 U.S. 488 (2009).....	4, 17, 24
<i>Susan B. Anthony List v. Driehaus</i> , 573 U.S. 149 (2014).....	20, 25
<i>Texas v. United States</i> , 523 U.S. 296 (1998).....	28
<i>TransUnion LLC v. Ramirez</i> , 141 S.Ct. 2190 (2021).....	19
<i>Trump v. Wis. Elections Comm'n</i> , 983 F.3d 919 (7th Cir. 2020).....	16

<i>Tyler v. Cuomo</i> , 236 F.3d 1124 (9th Cir. 2000).....	36
<i>United States v. Classic</i> , 313 U.S. 299 (1941).....	15, 23
<i>United States v. Fortner</i> , 455 F.3d 752 (7th Cir. 2006).....	34
<i>United States v. Students Challenging Regulatory Agency Procedures</i> , 412 U.S. 669 (1973)	5
<i>Verizon Md., Inc. v. Pub. Serv. Comm’n of Md.</i> , 535 U.S. 635 (2002).....	5, 32
<i>Warth v. Seldin</i> , 422 U.S. 490 (1975).....	35
<i>Wearry v. Cain</i> , 577 U.S. 385 (2016).....	35
<i>West Virginia v. EPA</i> , 142 S.Ct. 2587 (2022).....	30
<i>Wood v. Raffensperger</i> , 981 F.3d 1307 (11th Cir. 2020).....	27
<i>Yick Wo v. Hopkins</i> , 118 U.S. 356 (1886).....	37
Statutes	
U.S. CONST. art. I, § 4.....	2, 14, 27-28, 32-35
U.S. CONST. art. II, § 1, cl. 2.....	2, 14, 27-28, 32-35
U.S. CONST. art. III.....	3-4, 13-19, 22-27, 34, 36-38
U.S. CONST. amend. V, cl. 4	27
U.S. CONST. amend. XI.....	31-32
U.S. CONST. amend. XIV, §1, cl. 3.....	32-33
28 U.S.C. §1254(1).....	1
28 U.S.C. §1291	1
28 U.S.C. §1331	1, 31
28 U.S.C. §1343	1, 33

28 U.S.C. §1343(3).....	33
28 U.S.C. §1343(4).....	33
28 U.S.C. §1367	1, 33
28 U.S.C. §1653	5-6, 12, 17, 20, 34, 36
42 U.S.C. §1983	31, 33
42 U.S.C. §1988(a).....	33
Civil Rights Act of 1871, 17 Stat. 13.....	31
Judiciary Act of 1875, 18 Stat. 470.....	31
A.R.S. §16-442(A)-(C)	12
A.R.S. §16-442(B)	8
A.R.S. §16-449(A)	17
A.R.S. §16-452(C)	17
A.R.S. §16-1004(B)	17
A.R.S. §16-1009	12, 17
A.R.S. §16-1010	12, 17
Rules, Regulations and Orders	
S.Ct. R. 21.....	12
S.Ct. R. 22.....	12
FED. R. CIV. P. 11.....	12
FED. R. EVID. 201(d)	11, 17
Other Authorities	
Richard C. Chen, <i>Summary Dispositions as Precedent</i> , 61 WM. & MARY L. REV. 691 (2020) ..	34
Jennifer Ann Drobac, <i>The Misappropriation, Embezzlement, Theft, and Waste of Corporate Human and Financial Assets: Sexual Harassment Reconceived</i> , 36 ABA JOURNAL LAB. & EMP. LAW 425 (2022)	18
2 M. Farrand, RECORDS OF THE FEDERAL CONVENTION OF 1787 (1911)	37

PETITION FOR WRIT OF CERTIORARI

Kari Lake and Mark Finchem respectfully petition this Court for a writ of *certiorari* to the U.S. Court of Appeals for the Ninth Circuit to review the dismissal of their case. Respondents are Arizona’s Secretary of State and the boards of supervisors of Maricopa and Pima Counties in their respective official capacities.

OPINIONS BELOW

The Ninth Circuit’s *per curiam* opinion is reported at 83 F.4th 1199 and reprinted in the Appendix (“App”) at App:1a. The district court’s order dismissing the case is reported at 623 F.Supp.3d 1015 and reprinted at App:10a.

JURISDICTION

On October 16, 2023, the Ninth Circuit affirmed the dismissal of the case. By order dated February 5, 2024, the Circuit Justice extended the time within which to petition this Court to March 14, 2024. *In re Lake*, No. 23A622 (2024). The district court had jurisdiction under 28 U.S.C. §§1331, 1343, 1367, and the Ninth Circuit had jurisdiction under 28 U.S.C. §1291. This Court has jurisdiction under 28 U.S.C. §1254(1).

STATUTORY PROVISIONS INVOLVED

The Appendix (“App.”) contains the relevant statutory and regulatory provisions.

STATEMENT OF THE CASE

Public distrust in elections is at an all-time high and growing. As 2022 candidates for Governor and Secretary of State, petitioners filed this action in advance of the election to challenge Arizona’s electronic voting machines’ suitability to assure fair and accurate votes consistent with the Constitution.

Although electronic voting machines were meant to remedy snafus like the 2000 Florida recount, the flaws that petitioners unearthed in electronic voting machines make hanging chads—the very problem the machines were meant to solve—seem like a blessing. At least there, humans could see and touch ballots and punch cards. By turning elections over to black boxes running software outside the public domain, we surrendered the ability to meaningfully verify the election process.

Newly uncovered evidence also shows Arizona’s Maricopa County flagrantly violated state law for electronic voting systems—including using altered software not certified for use in Arizona—and actively misrepresented and concealed those violations. Perhaps worse—although potentially unknown to Maricopa—the Dominion Voting Systems, Inc., systems used in Maricopa and almost thirty states have a built-in security breach enabling malicious actors to take control of elections, likely without detection.

Importantly, this Court has a hand both in the problem and a solution. Institutional inertia from having intervened in the 2000 election should not sideline this Court’s review of new systemic flaws in our elections. Indeed, the Court’s recent decisions have created a “Goldilocks problem” that only this Court can resolve. On the too-cold side, *Lance v. Coffman*, 549 U.S. 437 (2007), has come to stand for the proposition voters cannot assert claims under the Elections and Electors Clauses. On the too-hot side, *Purcell v. Gonzalez*, 549 U.S. 1 (2006), posits that election-law challenges brought by candidates—once the candidates are known—come too close to elections. Cases are never “just right” for voters or candidates to

challenge the wholesale bombardment of States' election-integrity laws or practices that decide close elections.

Georgia's *Curling* litigation aptly illustrates this conundrum. In *Curling*, the district court denied an injunction against use of ballot marking devices ("BMDs") to vote in Georgia because the election was just weeks away, but acknowledged that plaintiffs' national security experts "convincingly" showed vote manipulation with these machines "was not a question of 'might this actually ever happen?'— but 'when it will happen.'" *Curling v. Raffensperger*, 494 F.Supp3d 1264, 1342 (N.D. Ga. 2020). Three years later, the district court denied in part defendants' motion for summary judgement. *Curling v. Raffensperger*, __ F.Supp.3d __, 2023 U.S. Dist. LEXIS 202368 (N.D. Ga. Nov. 10, 2023). After a trial earlier this year, a decision on the constitutionality of using BMDs is pending. Meanwhile, two elections took place in 2020 and 2022 in Georgia with profound national implications. The Georgia BMD software that could be manipulated "to steal votes" according to the *Curling* plaintiffs' expert is essentially what Maricopa uses. App:90a-94a (¶¶130-140).

The solution is simple: this Court must confine *Lance* to its actual holding—namely, election-related challenges that assert no voting right or other Article III interest are generalized grievances outside federal jurisdiction. But election-related challenges asserting injuries to voting rights—even widely shared injuries—can be justiciable.

To restore faith in elections, this Court must take two simple actions.

- *First*, the Court should summarily reverse here, while limiting *Lance* to its actual holding.
- *Second*, as part of implementing *Moore v. Harper*, 143 S.Ct. 2065 (2023), the Court should commit to taking on an error-correcting role for justiciability in election challenges, at least until lower courts understand what Article III covers and what it does not cover.

As *Moore* has now held, the federal Constitution allows federal-court oversight of efforts to neuter State election laws for electoral advantage. Even where dismissal under Article III is correct, the dismissal decision needs to address plaintiffs' position rather than facilely citing *Lance*. App:7a. The public requires more, and the courts should not withhold it.

I. LEGAL BACKGROUND

Three justiciability issues underlie this petition: (1) the contours of Article III standing, (2) exceptions to the States' sovereign immunity, and (3) plaintiffs' ability to make new allegations of jurisdiction on appeal.

A. Standing under Article III

Standing's tripartite test requires: (a) judicially cognizable injury to plaintiffs, (b) causation by the challenged conduct, and (c) redressability by courts. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561-62 (1992). Injury must be actual or imminent, not merely speculative, conjectural, or hypothetical. *Summers v. Earth Island Institute*, 555 U.S. 488, 493 (2009). Further, injury must be "concrete and particularized" to the plaintiff, not an "abstract generalized grievance suffered by all citizens." *Carney v. Adams*, 141 S.Ct. 493, 498-99 (2020). The requirement for injury "serves to distinguish a person with a direct stake in the

outcome of a litigation—even though small—from a person with a mere interest in the problem.” *United States v. Students Challenging Regulatory Agency Procedures*, 412 U.S. 669, 689 n.14 (1973) (“*SCRAP*”).

Causation and redressability pose “little question” when the government directly regulates a plaintiff, although standing requires a heightened showing when the government regulates third parties, who then cause injury. *Lujan*, 504 U.S. at 561-62. Moreover, to establish subject-matter jurisdiction, a complaint’s “general allegations embrace those specific facts that are necessary to support the claim.” *Bennett v. Spear*, 520 U.S. 154, 168 (1997). The following subsections demonstrate petitioners’ cognizable injuries, causation, and redressability.

B. Sovereign Immunity and *Ex parte Young*

Sovereign immunity bars suits against States in federal court, but the *Ex parte Young* officer-suit exception allows suits in which the plaintiff seeks only prospective injunctive or declaratory relief regarding ongoing violations of federal law. Courts conduct a “straightforward inquiry into whether the complaint alleges an ongoing violation of federal law and seeks relief properly characterized as prospective.” *Verizon Md., Inc. v. Pub. Serv. Comm’n of Md.*, 535 U.S. 635, 645 (2002) (interior quotations omitted). Without an ongoing violation of federal law, *Young* may not apply. *Id.*; *Green v. Mansour*, 474 U.S. 64, 66-67 (1985).

C. Amended Jurisdictional Allegations under 28 U.S.C. §1653.

Under 28 U.S.C. §1653, allegations of jurisdiction can be amended, even on appeal, if the jurisdictional facts existed when the operative complaint was filed. *Newman-Green, Inc. v. Alfonzo-Larrain*, 490 U.S. 826,

830-32 (1989). Thus, where “jurisdiction ... actually exists,” parties can cite that jurisdiction for the first time on appeal. *Id.* at 831. Relatedly, failure to raise jurisdictional arguments does not waive those arguments. *Sochor v. Florida*, 504 U.S. 527, 534 n.* (1992). Although the jurisdictional issues in *Newman-Green* were different, the Court relied on the value of avoiding the “needless waste of time” for litigants and courts to start over in district court, which “runs counter to effective judicial administration.” *Newman-Green*, 490 U.S. at 833 (internal quotation omitted). Even without *res judicata* or fraud on the court concerns, requiring parties to start over in district court for “hypertechnical jurisdictional purity” would harm the legal system and deny important rights. *Id.* at 837-38.

II. FACTUAL BACKGROUND

The bases for petitioners’ standing is stated in their complaint, district court declarations and hearing testimony, and amended allegations of jurisdiction made here pursuant to 28 U.S.C. § 1653 based on discovery in other matters and public-record requests that were not known until after the Ninth Circuit order affirming dismissal of the amended complaint.

Petitioners brought this action alleging concrete facts showing that the *existing* state of Arizona’s electronic voting machines posed a definable and substantial risk of election manipulation and an inability to deliver accurate and trustworthy results. Vast majorities of both voters and election workers do not understand how these machines work or whether the reported results are truly accurate. Instead, the accuracy of elections results depends on blindly

trusting private companies who sell and service these machines, while refusing to make their software available to neutral expert evaluation. App:49a, 51a, 62a-64a (¶¶2, 8, 63-64, 69-70). The machines are easily compromised, and their security safeguards are easily bypassed or defeated, and shown to deliver inaccurate results. App:55a-56a, 65a-82a, 88a-91a (¶¶27, 30-31, 72-107, 125-134). They contain critical parts made in countries like China that are known adversaries that routinely use components, such as motherboards and microchips, to surreptitiously access computer systems. App:75a-76a (¶¶91-92). The question is not how many times inaccurate results were discovered, but rather how many times have they not.

A. The record before the district court.

In addition to their complaint's allegations, petitioners also moved for a preliminary injunction, with six qualified cyber experts testifying concerning the voting machines' unsuitability to provide a secure and accurate vote. App: 144a, 151a-154a. The expert testimony and evidence showed actual vote manipulation in prior Maricopa and Pima elections, as well as in other jurisdictions.

Petitioners' complaint overlaps with the claims brought in *Curling, supra*, to prohibit the use of electronic BMDs in Georgia, which went to trial in January, and a decision is pending. App:49a-50a, 93a-95a. (¶¶4, 139-140, 146).

1. The complaint's allegations.

The complaint pled detailed particularized facts casting substantial doubt on whether the existing state of Arizona's electronic voting machines likely

could produce accurate election results. The complaint included well-pled allegations that:

- All Arizona-certified optical scanners and ballot marking devices, as well as the software on which they rely, have been wrongly certified for use in Arizona because they do not comply with the statutory requirements set forth at A.R.S. §16-442(B), making these systems easily vulnerable to manipulation. App:54a, 91a-94a (¶¶23, 135-143).
- An independent post-2020 election audit of Maricopa’s electronic voting machines found an 11,592-ballot discrepancy between the official result totals and the equivalent Final Voted File’s totals, demonstrating an inability to reconcile votes. App:64a (¶70).
- Congressional and other government officials’ warnings that Arizona’s registration system was actually hacked in 2016 and the vulnerabilities remained unremedied. App:69a-70a, 76a-77a (¶¶79, 94).
- Maricopa election officials did not have the credentials necessary to validate tabulator configurations and independently validate the voting system prior to an election. The vendor, Dominion, had those credentials, and *refused the Arizona Senate’s subpoena* to produce those passwords in connection with the Senate’s investigation of these voting machines. App:62a, 95a (¶¶63, 148-49).
- Despite certifications by the Election Assistance Commission (“EAC”), voting machines like those used in Arizona have been hacked, manipulated, or failed to record votes accurately on multiple

occasions. App:65a-82a, 65a-82a, 88a-91a (¶¶30, 72-107, 125-134).

- Recognized experts have shown 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. App:56a. 94a-95a (¶¶31, 144-146).

As voters and political candidates, petitioners thus adequately pled the likelihood of a cognizable future injury from not counting votes accurately.

2. The preliminary injunction evidence.

In connection with their motion for a preliminary injunction against using Arizona’s electronic voting machines, petitioners introduced declarations and testimony from six credentialed cyber and national security experts. They all testified that electronic voting systems could be easily breached and manipulated.

Notably, petitioners introduced the sworn declaration of Dr. Walter Daugherity, a longstanding professor—now emeritus—in the Department of Computer Science and Engineering at Texas A&M University. He examined of the Cast Vote Records for seventeen races in Pima County and ten races Maricopa County for the 2020 election. App:114a-115a (¶¶6-9). His analysis showed that “in the November 2020 election for which the CVR data was made available, ballots in Maricopa County and Pima County were artificially processed through the tabulators tracking a Proportional-Integral-Derivative (PID) type control function in a closed-loop feedback system.” App:114a (¶7). Dr. Daugherity

testified “that after about 12% of the early votes are recorded, the next block of ballots is 75% for the Democrat candidate, the next block after that is 74%, the next block 73%, and so on, systematically declining all the way to Election Day” App:121a (¶30). He concluded that “[s]uch predictability and dependence would not occur without artificial manipulation.” App:56a (¶31). Respondents did not rebut this analysis. Afterwards, Maricopa produced CVR data in randomized form, preventing similar analyses of subsequent elections.

At the preliminary-injunction hearing, cyber expert Clay Parikh testified that he had performed “a hundred or more security tests” on electronic voting machines, like those used in Arizona, while performing EAC certification tests. App:155a. Parikh testified it took him “[o]n average, five to ten minutes” to hack these voting machines, including the voting machines like those used in Arizona. *Id.*

Another cyber expert, Ben Cotton, previously retained by the Arizona Senate to examine Maricopa’s electronic voting machines, testified about Maricopa’s reliance on an “air gapped” system to prevent remote hacking. He testified that “[i]n the case of Maricopa ... that air-gap system, given the configuration of those other components of the enterprise, could be bypassed in about 30 seconds.” App:147a. He also found “actual evidence of remote log-ins into [Maricopa’s] EMS server.” App:148a; *see also* App:150a (NSA’s “air gapped” system was breached).

This expert testimony—unrefuted by respondents and ignored by the Ninth Circuit, App:3a—showed additional concrete evidence of actual past ballot manipulation in Maricopa and Pima Counties

through the electronic voting machines and uncorrected systemic vulnerabilities going into the November 2022 election.

B. Maricopa’s chaotic 2022 election.

The district court dismissed Petitioner’s complaint on August 26, 2022, ruling that Petitioner’s claims were “too speculative” to support standing. App:29a. On Election Day, November 8, 2022, Maricopa experienced a massive disruption with its electronic voting machines. Evidence from Maricopa’s tabulator system log files presented to the Arizona Senate Committee on Elections showed that on Election Day, Maricopa’s vote center tabulators rejected over 7,000 ballots *every thirty minutes* beginning almost immediately after the vote centers opened at 6:00 am and continuing past 8:00 pm—totaling over 217,000 rejected ballot insertions on a day when approximately 248,000 votes were cast.¹

C. New evidence of misconduct in prior elections.

Petitioners recently obtained system log (“SLOG”) files from Maricopa’s 2020 election that are at odds with Maricopa’s statements to the district court with respect to material facts on which the district court relied in dismissing petitioners’ claims for lack of standing. Based on that new information, petitioners

¹ <https://www.azleg.gov/videoplayer/?eventID=2023011091> at 2:00:30, 2:13:20-2:14:37 (last visited Mar. 14, 2024). Publicly available records on the Legislature’s website are judicially noticeable. *Pedersen v. Bennett*, 230 Ariz. 556, 559, ¶15 (2012); FED. R. EVID. 201(d).

seek to amend their allegations of jurisdiction under 28 U.S.C 1653. Specifically, the SLOG files show:²

- In place of the Arizona-certified election software that Maricopa claimed to use, Maricopa’s election software has been surreptitiously altered with respect to components controlling how ballots are read and tabulated. The election results put through this uncertified software are unreliable. Contrary to Maricopa’s representations to the district court, the election software Maricopa used in the 2020 election is not approved by the EAC or for use in Arizona in violation of Arizona law.³ The SLOG files show that Maricopa used the same uncertified software in the 2022 election.
- Contrary to Maricopa’s representations to the district court, Maricopa did not conduct statutorily mandated pre-election logic and accuracy (“L&A”) testing prior to the November 2020 election on all its vote center tabulators. Instead, Maricopa L&A tested only five spare tabulators. Maricopa did the same thing in connection with the November 2022 election.

The district court relied on these false representations in dismissing petitioners’ complaint, App:18a-19a, and in finding that sanctions should be awarded against plaintiffs under Rule 11.

Further, in Dominion’s contract with Maricopa—and its contracts with other counties nationwide—

² In a separate filing, petitioners will submit the new evidence in support of seeking further relief from the Court—or Circuit Justice—pursuant to Rules 21 or 22.

³ A.R.S. §16-442(A)-(C). Indeed, the unapproved alteration of election software is criminal. A.R.S. §§16-1009, 16-1004(B), 16-1010.

Dominion commits to protecting election data with high-level Federal Information Processing Standard (“FIPS”) level encryption. New evidence shows that, since at least 2020, Dominion configured its machines with the decryption keys in an election database table in plain text—protected by nothing other than Windows log-in credentials that are easily bypassed—enabling any malicious actor total control over its electronic voting systems. This security breach violates *common sense*, to say nothing of FIPS-level encryption. While this breach has the game-changing *magnitude* of the Allies’ deciphering Germany’s ENIGMA machine in World War II, it is far worse. Dominion leaves the decryption keys bare, in plain text.

Embedded Dominion employees or any malicious actor who knows where to look can gain total access and control over an election. It is like a bank telling the public they have the most secure vault in the world, and then taping the combination on the wall next to the vault door. Even worse, key logging features that would record system activity showing such control can also be manipulated or disabled, thereby rendering any penetration of this system nearly undetectable.

III. PROCEDURAL BACKGROUND

The Ninth Circuit affirmed the district court’s dismissal of this action for lack of Article III standing on the theory that the claim of injury is speculative. App:3a. The district court based its dismissal on two additional grounds (sovereign immunity and temporal issues for the 2022 election under *Purcell*). App:32a-37a. Petitioners requested that—if their complaint was inadequate—they be allowed to amend to include

the preliminary-injunction evidence, Pls.' Opp'n 17 (ECF #58), but the Ninth Circuit did not consider that evidence in determining whether injury was non-speculative. App:3a.

REASONS TO GRANT THE WRIT

The petition raises critical issues on Article III standing in the election context, as well as issues of Due Process, voting rights, and ballot integrity. This Court should grant the writ of *certiorari* for several independent reasons.

1. The lower courts' disregard of petitioners' claims conflicts with other circuits—and even the Ninth Circuit—on standing for election challenges. *See* Section I.A.1.c(1), *infra*.
2. The lower courts have taken *Lance* beyond its limited holding to deny voter standing for Elections and Electors Clause claims. *See* Section I.A.5.b, *infra*.
3. The Circuits are split on the justiciability of claims under the Elections and Electors Clauses, which *Moore* and the upcoming 2024 election make urgent. *See* Section I.A.5.b, *infra*.
4. This litigation offers the opportunity to address critical faults in election infrastructure before the 2024 election. *See* Section III, *infra*.

Petitioners respectfully submit that each of these issues warrants not only granting a writ of *certiorari* but also resolving this matter on an expedited basis or summarily.

I. THE DISTRICT COURT HAD AND STILL HAS JURISDICTION TO RESOLVE THIS ACTION.

In addition to reviewing the Ninth Circuit's Article III basis for affirming the district court's

dismissal, this Court can review any basis for dismissal that is supported in the record, *Dittman v. California*, 191 F.3d 1020, 1027 n.3 (9th Cir. 1999), because “there is no unyielding jurisdictional hierarchy” to threshold bases for dismissal. *Ruhrgas Ag v. Marathon Oil Co.*, 526 U.S. 574, 578 (1999).

Appellate courts’ sound discretion guides the decision on whether to reach issues not decided below. *Singleton v. Wulff*, 428 U.S. 106, 121 (1976). This Court should reach—and can easily decide—the sovereign immunity and *Purcell* issues raised in the district court. Without resolving those issues, reversal on Article III and remand to the district court might be a pyrrhic—and short lived—victory, requiring yet another appeal.

A. Petitioners had and still have Article III standing.

For the paramount public function of running elections, Maricopa uses uncertified voting systems controlled by private actors and susceptible to hacking, evades required testing, and makes misrepresentations when called to task. It is no surprise that public confidence in election integrity is at all-time lows. All these factors bolster petitioners’ standing to sue.

As both voters and candidates, petitioners have standing to challenge Maricopa’s election procedures to redress several cognizable injuries:

- *For voters*, Maricopa’s elections are so unreliable and open to abuse as to nullify the fundamental, due process right to vote and to have votes accurately counted. *United States v. Classic*, 313 U.S. 299, 315 (1941) (“included within the right to choose, secured by the Constitution, is the right of

qualified voters within a state to cast their ballots and have them counted”); *Stewart v. Blackwell*, 444 F.3d 843, 868-69 (6th Cir. 2006) (collecting cases); see Section I.A.1.c(1), *infra*.

- *For candidates*, Maricopa’s elections inflict not only unequal-footing injuries that deny the right to run for public office under lawful and reliable competitive elections, *Mecinas v. Hobbs*, 30 F.4th 890, 897-900 (9th Cir. 2022); *Trump v. Wis. Elections Comm’n*, 983 F.3d 919, 924 (7th Cir. 2020), but also—by increasing public distrust in elections, *Purcell*, 549 U.S. at 4 (“[v]oter fraud drives honest citizens out of the democratic process and breeds distrust of our government”)—make it more difficult and more expensive for candidates to get voters to vote, forcing candidates to spend more time fundraising and less time campaigning, thereby inflicting First Amendment associational injuries, *Krislov v. Rednour*, 226 F.3d 851, 857 (7th Cir. 2000) (being “required to allocate additional campaign resources ... in itself can be an injury to First Amendment rights”), beyond the financial and unequal-footing injuries. See Section I.A.1.c(2), *infra*.

As explained in this subsection, these injuries easily meet the criteria of Article III.

1. Petitioners suffer particularized and concrete injury from Maricopa’s unlawful election practices.

Petitioners have suffered and still suffer particularized, concrete injuries from Maricopa’s unlawful election policies and execution. Moreover, because petitioners suffer these concrete injuries, they also have standing to challenge *procedural*

injuries from procedural violations of election law. *See Summers*, 555 U.S. at 496; Section I.A.2, *infra*. Significantly, these injuries persist as to *future* elections, even if this case became moot as to the 2022 election.

a. This Court can consider new allegations related to standing.

As indicated in the Legal Background, §1653 allows parties to seek to amend allegations of jurisdiction, even on appeal. *See* page 5, *supra*; 28 U.S.C. §1653; *cf.* FED. R. EVID. 201(d) (judicially noticeable government documents admissible on appeal). Based on new evidence Maricopa’s pre-existing election practices, petitioners seek to make the following additional allegations regarding standing:

- *First*, Maricopa did not conduct the required L&A testing, on which the district court relied to find the risk of election interference speculative.
- *Second*, Maricopa did not use certified software, on which the district court relied to find the risk of election interference speculative.
- *Third*, Maricopa used software that made all passwords needed to control Maricopa elections available to anyone with physical or remote access, which supports petitioners’ allegations and evidence that past elections were manipulated.
- *Fourth*, altering election software without the Arizona Secretary of State’s approval is criminal act under Arizona law, A.R.S. §§16-449(A), 16-452(C), 16-1009, 16-1004(B), 16-1010, thereby evaporating presumptions in their favor under Arizona law. *See* note 5, *infra* (Arizona’s “bursting bubble” theory of nonstatutory presumptions).

- *Fifth*, Maricopa’s officials misrepresented their compliance with Arizona election law (e.g., L&A testing, certified software), which negates any presumptions in their favor under Arizona law. *See* note 5, *infra* (Arizona’s “bursting bubble” theory of nonstatutory presumptions).
- *Sixth*, Maricopa officials abdicated control over the complex election systems to embedded private Dominion employees who lack any presumption of regularity under Arizona law. *See* note 4, *infra*.

These allegations of jurisdiction all pre-date this lawsuit and thus support a finding of jurisdiction here.

The new allegations meet the tripartite test of “motive, means and opportunity” that “can result in [a] perfect storm of conditions leading to embezzlement” or fraud. Jennifer Ann Drobac, *The Misappropriation, Embezzlement, Theft, and Waste of Corporate Human and Financial Assets: Sexual Harassment Reconceived*, 36 ABA JOURNAL LAB. & EMP. LAW 425, 463 (2022) (internal quotation omitted). Together, these three “warning signs ... can go a long way toward identifying and thwarting an ongoing fraud.” *Id.* (internal quotation omitted). Moreover, neither private actors like embedded Dominion employees⁴ nor Arizona election officials

⁴ Arizona election officials benefit from nonstatutory presumptions of regularity, *Hunt v. Campbell*, 19 Ariz. 254, 268 (1917), but those presumptions do not apply to private actors engaged in an election. *Garcia v. Sedillo*, 70 Ariz. 192, 200 (1950) (“the officials in this election were not public officials where we can say that there is a presumption that they acted in good faith”).

who commit misconduct⁵ enjoy a presumption of regularity. These factors coupled with the evidence and allegations supporting Article III injury easily establish enough likelihood of future injury to survive dismissal for lack of an Article III controversy.

b. Petitioners' injuries are actual and imminent, not speculative.

The Article III imminence requirement does not require that petitioners wait to be injured. *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2210 (2021). Indeed, in the election context, such a standard is unworkable. Instead, imminence for “risk of future harm” requires only a “risk of harm [that] is sufficiently imminent and substantial.” *Id.* That standard is met here for several reasons.

- *First*, procedural injury lowers the Article III threshold for immediacy, *see* Section I.A.2, *infra*, which applies whenever government violates election procedures.
- *Second*, and relatedly, unequal-footing injuries occur upon denying lawful competition, not in denying the ultimate benefit. *See Northeastern Fla. Chapter of Associated Gen. Contractors of Am. v. City of Jacksonville*, 508 U.S. 656, 666 (1993); Section I.A.1.c, *infra*. For unequal-footing injuries, the ultimate benefit “is merely one of relief,” not one of injury. *Regents of the Univ. of California v. Bakke*, 438 U.S. 265, 280 n.14 (1978).

⁵ For election officials, nonstatutory presumptions evaporate in the face of rebuttal evidence: “Whenever evidence contradicting a legal presumption is introduced the presumption vanishes.” *Silva v. Traver*, 63 Ariz. 364, 368 (1945); *Golonka v. GMC*, 204 Ariz. 575, 589-90 ¶48 (App. 2003) (discussing Arizona’s “bursting bubble” treatment of presumptions).

- *Third*, under petitioners' complaint and evidence, and their new allegations of jurisdiction, 28 U.S.C. §1653, the injury in past elections provides evidence of injury in future elections that the lower courts failed to consider. *See* Section I.A.3, *infra*.
- *Fourth*, when multiple actors can cause injury, the threat of injury is increased. *Compare Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 164 (2014) with *Curling*, __ F.Supp.3d at __, 2023 U.S. Dist. LEXIS 202368, at *120 (“Mueller Report’s findings leave no doubt that Russia and other adversaries will strike again”) (alterations and internal quotation omitted) (No. 1:17-cv-2989-AT).
- *Fifth* for cybersecurity injuries outside of elections (*e.g.*, regarding fiduciary obligations to protect money or personal information), courts easily find imminence *vis-à-vis* improper actions that injure plaintiffs. *See, e.g., Lewert v. P.F. Chang's China Bistro, Inc.*, 819 F.3d 963, 967-68 (7th Cir. 2016) (victims need not wait for identity theft to happen). As is the case with the hacking of personal information, bad actors in this case have committed crimes by positioning Maricopa elections in their current non-compliant state. A court should not assume that the bad actors did so benevolently. *See* notes 4-5, *supra* (presumptions of regularity do not apply). All civil and criminal rights depend upon honest elections, *Reynolds v. Sims*, 377 U.S. 533, 562 (1964), and, therefore, courts should treat voting rights at least as well as personal privacy.

All these reasons—ignored by the lower courts—establish non-speculative risk of future injury.⁶ Indeed, Maricopa’s 2022 election was a disaster, based on flaws in the voting machines.

c. Petitioners’ injuries are concrete and particularized, not abstract or generalized.

The widely shared nature of the injury does not foreclose finding an injury particularized to a given plaintiff:

Often the fact that an interest is abstract and the fact that it is widely shared go hand in hand. But their association is not invariable, and where a harm is concrete, though widely shared, the Court has found “injury in fact.”

FEC v. Akins, 524 U.S. 11, 24 (1998); *Gill v. Whitford*, 138 S.Ct. 1916, 1929 (2018) (right to vote is personal and individual). Moreover, “intangible injuries can nevertheless be concrete,” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 340 (2016), if they affect a plaintiff “in a personal and individual way.” *Id.* at 339. Here, the injury to voting rights is both concrete and particularized.

In *Akins*, an “informational injury ... related to voting, the most basic of political rights, [was] sufficiently concrete and specific,” *Akins*, 524 U.S. at 24-25; *accord Robins*, 578 U.S. at 339 n.7, notwithstanding that it was also widely shared. Indeed, *Akins* used the example “where large numbers of voters suffer interference with voting rights conferred by

⁶ The purported “air-gapped” Maricopa system provides no significant protection from outside intrusion, App: 153a, and even less from inhouse actors who lack a presumption of regularity. See notes 4-5, *supra*.

law.” *Akins*, 524 U.S. at 24. As *Akin* hypothesized, the injury here falls on voting itself. As such, Maricopa’s actions nullify each voter’s fundamental right to vote.

(1) Candidates and political parties suffer injury.

As with voters’ due process right to have their votes counted accurately, “inaccurate vote tally is a concrete and particularized injury to candidates.” *Carson v. Simon*, 978 F.3d 1051, 1058 (8th Cir. 2020). But candidates and political parties may have greater interests in election-law compliance than individual voters based on running in a competitive environment and seeking to ensure an equal-footing *vis-à-vis* other candidates and political parties. *See, e.g., Mecinas*, 30 F.4th at 897-900 (finding that political parties have competitor standing to challenge allegedly unlawful election regulations); *accord Fulani v. League of Women Voters Educ. Fund*, 882 F.2d 621, 626 (2d Cir. 1989); *cf. Clinton v. City of New York*, 524 U.S. 417, 433 n.22 (1998) (unequal-footing injuries apply outside equal-protection context). While candidates are themselves voters and political parties are membership organizations whose members are voters, parties and candidates have interests in a fair competition that voters may lack.

Further, like states, candidates and parties have cognizable interests in avoiding fraud to ensure voter confidence in election integrity, *Crawford v. Marion County Election Bd.*, 553 U.S. 181, 189 (2008), as a means of keeping “honest citizens [in] the democratic process.” *Purcell*, 549 U.S. at 4. Reaching disengaged constituents requires more effort and expense, which is its own Article III injury. *Shays v. FEC*, 414 F.3d

76, 90-91 (D.C. Cir. 2005) (relying on “basic economic logic” to find standing) (interior quotation omitted).

Finally, increasing candidates’ effort and expense to get out the vote forces them to spend more time fundraising and less time campaigning, inflicting First Amendment associational injuries, *Krislov*, 226 F.3d at 857; *accord Nader v. Blackwell*, 545 F.3d 459, 472 (6th Cir. 2008). Although they were 2022 candidates when the complaint was filed, petitioners are 2024 candidates now.

(2) Voters suffer injury.

Voters suffer injury when election-law violations deny them of an accurate vote count or allow unlawful votes to dilute their lawful votes: “[O]ne thing is clear: total and complete disenfranchisement of the electorate as a whole is patently and fundamentally unfair (and, hence, amenable to rectification in a federal court).” *Bonas v. Town of N. Smithfield*, 265 F.3d 69, 75 (1st Cir. 2001); *see also Classic*, 313 U.S. at 315; *Stewart*, 444 F.3d at 868-69 (collecting cases); *Shaw v. Reno*, 509 U.S. 630, 640-41 (1993) (“the right to vote can be affected by a dilution of voting power as well as by an absolute prohibition on casting a ballot”) (internal quotations and alteration omitted); *Reynolds*, 377 U.S. at 555. In any event, voters have standing to protect their voting rights:

We have allowed important interests to be vindicated by plaintiffs with no more at stake in the outcome of an action than a *fraction of a vote*, a \$ 5 fine and costs, and a \$1.50 poll tax.

SCRAP, 412 U.S. at 689 n.14 (citations omitted, emphasis added). As explained in Section I.A.5.b,

infra, *Lance*, on which the lower courts relied, is not to the contrary.

2. Petitioners’ procedural injuries lower the Article III threshold for immediacy and redressability.

Because Maricopa does not count votes via the required procedures that are in place to protect the accuracy of the vote, *see* Section I.A.1.a, *supra*, this action is based partly on *procedural* injury. Significantly, petitioners suffer concrete injuries to their fundamental right to vote and to fair elections, *see* Section I.A.1, *supra*, so this type of procedural injury lowers the Article III threshold for immediacy and redressability. *Lujan*, 504 U.S. at 571-72 & n.7 (a proper procedural-injury plaintiff “can assert that right without meeting all the normal standards for redressability and immediacy”); *cf.* *Summers*, 555 U.S. at 496 (plaintiffs must have concrete injury to assert procedural injury). Procedural-rights plaintiffs have standing for a “do-over” under the proper procedures and standards, even if the election might produce the same winners. *See Akins*, 524 U.S. at 25. Although the 2022 election had not yet occurred when petitioners filed the operative complaint or when the district court ruled, a court could order “do-over” relief (*e.g.*, counting the paper ballots) in the 2022 election, as well as similar relief in future elections. Neither immediacy nor redressability pose an Article III barrier here.

3. Past injuries are evidence of future injury.

The district court improperly rejected or ignored petitioners’ allegations of security breaches in past elections, App:55a-56a, 65a-82a, 88a-91a (¶¶27, 30-

31, 72-107, 125-134), which is itself reversible error. *See O’Shea v. Littleton*, 414 U.S. 488, 496 (1974) (“past wrongs are evidence bearing on whether there is a real and immediate threat of repeated injury”); *cf. Driehaus*, 573 U.S. at 164 (“history of past enforcement” is obvious evidence of “substantial” threat of future enforcement). With petitioners’ new evidence of pre-litigation security breaches in prior elections, the risk of similar harm in future elections is undeniable. *See* Section I.A.1.a, *supra*. While the lower courts may not have found that petitioners’ claims “[c]ross the line from conceivable to plausible,” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007), the new allegations—including that Maricopa misled the lower courts—clearly crosses the line, requiring courts to accept them as true against a motion to dismiss. *Lewert*, 819 F.3d at 967-68. Maricopa’s elections are simply not secure.

4. Petitioners’ injuries are traceable to Maricopa’s and the Secretary’s actions and redressable in court.

When petitioners filed this action, there was “little question” of causation or redressability because respondents directly injured petitioners, and a court could have stopped those injuries with injunctive relief. *See Lujan*, 504 U.S. at 561-62. The only question about causation and redressability now is whether petitioners’ injuries have now become impossible to redress. Even after elections have been held, however, their injuries would remain partially redressable by an injunction for *future* elections. *See*

Section I.C, *infra*.⁷ Accordingly, for Article III purposes, causation and redressability continue to pose “little question” here.

5. Petitioners’ standing covers any way that Maricopa violated election law.

Maricopa violated Arizona—and thus federal—election law in several ways. *See* Section I.A.1.a, *supra*. Once a plaintiff has standing to challenge unlawful government action, that same Article III controversy extends to any way in which the defendant violated the law.

a. Article III has no nexus requirement outside the Establishment Clause.

Because an Article III case or controversy exists here, *see* Section I.A.1.b, *supra*, petitioners can rely on the violation of any applicable constitutional or statutory provision: “once a litigant has standing to request invalidation of a particular [government] action, [the litigant] may do so by identifying all grounds on which the [government] may have failed to comply with its statutory mandate.” *DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 353 & n.5 (2006). Outside of taxpayer standing, there is no “nexus” requirement in the Court’s Article III decisions. *Duke Power Co. v. Carolina Evtl. Study Grp.*, 438 U.S. 59, 78-79 (1978). As such, petitioners can base their challenge on Arizona state election law unless barred by sovereign immunity and can base

⁷ For each form of requested relief, only one petitioner needs standing. *Massachusetts v. EPA*, 549 U.S. 497, 518 (2007) (“[o]nly one of the petitioners needs to have standing to permit us to consider the petition for review”).

their challenge on any federal law, even federal law that might not itself present a case or controversy.

Although standing to challenge one government action does not automatically provide standing to challenge other, discrete government actions, *Lewis v. Casey*, 518 U.S. 343, 358 n.6 (1996), standing doctrine has no general nexus requirement. *Duke Power*, 438 U.S. at 78-81. Thus, “once a litigant has standing to request invalidation of a particular agency action, it may do so by identifying all grounds on which the agency may have failed to comply with its statutory mandate.” *Cuno*, 547 U.S. at 353 & n.5 (interior quotations omitted). For example, in *Duke Power*, plaintiffs could use aesthetic injury from a new nuclear power plant (*e.g.*, algae blooms from releasing hot water into cooling ponds) to support a takings challenge to damage caps on *hypothetical future* catastrophic nuclear accidents. Article III is satisfied once a case or controversy exists on any basis related to the allegedly unlawful government action. Here, Maricopa not only altered election equipment and used uncertified software but also misrepresented the facts regarding those deviations from Arizona law. Just as the *Duke Power* plaintiffs could bring a Takings Clause claim by asserting aesthetic injuries, petitioners can bring an Elections Clause claim by asserting due-process injuries.

b. This Court should narrow *Lance* to its holding for voter standing under the Elections Clause.

Lance has wrongly come to stand for the proposition that voters cannot enforce the Elections and Electors Clauses. *See, e.g., Wood v. Raffensperger*, 981 F.3d 1307, 1314 (11th Cir. 2020) (affirming that if

the appellant had been a candidate for office “he could assert a personal, distinct injury” required for standing); *Bognet v. Sec’y Pa.*, 980 F.3d 336, 348-52 (3d Cir. 2020) (congressional candidate lacks standing under Elections Clause), vacated *sub nom. Bognet v. Degraffenreid*, 141 S.Ct. 2508 (2021); *Donald J. Trump for President, Inc. v. Sec’y Pa.*, 830 F.App’x 377, 387 (3d Cir. 2020); *Carson*, 978 F.3d at 1058. To the contrary, *Lance* merely held that generalized grievances cannot support standing for plaintiffs who lacked “the sorts of injuries alleged ... in voting rights cases.” *Lance*, 549 U.S. at 442. Voting-rights plaintiffs with standing on due-process or equal-protection grounds may identify all grounds on which an election failed to comply with applicable laws. See Section I.A.5.a, *supra* (standing has no general “nexus” requirement). Unlike the *Lance* plaintiffs, petitioners raised voting-rights injury, so *Lance* is inapposite.

B. This action was and remains ripe.

In addition to having standing, petitioners must also have a ripe claim. “A claim is not ripe for adjudication if it rests upon contingent future events that may not occur as anticipated, or indeed may not occur at all.” *Texas v. United States*, 523 U.S. 296, 300 (1998) (internal quotations and citations omitted). Because petitioners are *already suffering* concrete injury, see Section I.A.1.b, *supra*, their claims are also constitutionally ripe. Indeed, their procedural “claim[s] can never get riper.” *Ohio Forestry Ass’n v. Sierra Club*, 523 U.S. 726, 737 (1998) (procedural claims are fully formed at the procedural violation and “can never get riper”); see Section I.A.2, *supra*.

C. This action is not moot.

“A case becomes moot ... only when it is impossible for a court to grant any effectual relief whatever.” *Campbell-Ewald Co. v. Gomez*, 577 U.S. 153, 161 (2016) (internal quotations omitted). Significantly, although plaintiffs bear the burden of proving standing, defendants bear the burden of proving mootness. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 190 (2000). Under that burden, “the prospect that a defendant will engage in (or resume) harmful conduct may be too speculative to support standing, but not too speculative to overcome mootness.” *Id.* at 190. This Section demonstrates that petitioners’ action is not moot for two reasons.

1. As voters and future candidates, petitioners still suffer injury redressable in future elections.

Nothing in petitioners’ complaint limited relief to the 2022 election. Under *Campbell-Ewald*, it remains possible to issue relief for the 2024 and subsequent elections, which petitioners continue to seek. This case is not moot.

2. Even a complaint directed against only the 2022 election could avoid mootness as capable of repetition yet evading review.

Although the complaint was not directed solely against the 2022 election, App:110a (¶1), even a complaint so confined would not be moot under the “capable-of-repetition” exception to mootness. *Kingdomware Techs., Inc. v. United States*, 579 U.S. 162, 170 (2016) (interior quotation marks, citations, and alterations omitted). This exception obviously

applies “in the context of election cases ... when there are ‘as applied’ challenges as well as in the more typical case involving only facial attacks.” *FEC v. Wisconsin Right to Life, Inc.*, 551 U.S. 449, 463 (2007) (internal quotations omitted). Petitioners obviously will be voters in future elections and—indeed—are each candidates in the 2024 election.

Nor would any corrective action by either Arizona or Maricopa moot this action. Defendants who claim “mootness” must meet the “formidable burden of showing that it is absolutely clear the allegedly wrongful behavior could not reasonably be expected to recur.” *Friends of the Earth*, 528 U.S. at 190; *accord West Virginia v. EPA*, 142 S.Ct. 2587, 2607 (2022) (voluntary cessation does not moot a case without absolute clarity that the defendant could not resume the wrongful conduct). While Maricopa cannot meet that test, even curative Arizona legislation would not moot this action. *Diffenderfer v. Cent. Baptist Church, Inc.*, 404 U.S. 412, 415 (1972) (citations omitted, emphasis added); *accord Spomer v. Littleton*, 414 U.S. 514, 522-23 (1974). This action is not moot, and it will not become moot.

D. There is no “*Purcell* problem” for future elections.

Although the Ninth Circuit did not reach the issue, App:_9a, the district court dismissed on the alternate basis that petitioners brought this action too close in time to the 2022 election. *Compare* App:35a-37a *with Purcell*, 549 U.S. at 4-5 (out of concern for “voter confusion and consequent incentive to remain away from the polls,” federal courts avoid enjoining state election laws close to elections). While *Purcell* and its progeny may have counseled against providing

relief *vis-à-vis* the 2022 election, the complaint applied to future elections, so *Purcell* provides no basis for outright *dismissal*,

E. Sovereign immunity poses no barrier.

Similarly, although the Ninth Circuit did not reach the issue, App:9a, the district court dismissed on the alternate basis of sovereign immunity. Here, too, the Court should resolve this issue rather than allow respondents to reassert immunity on remand to the district court.⁸

By way of background, “two [post-Civil War] statutes, together, after 1908, with the decision in *Ex parte Young*, established the modern framework for federal protection of constitutional rights from state interference.” *Perez v. Ledesma*, 401 U.S. 82, 106-07 (1971). First, the Civil Rights Act of 1871, 17 Stat. 13, provided what now are 42 U.S.C. §1983 and 28 U.S.C. §1343(3). *Id.* Second, the Judiciary Act of 1875, 18 Stat. 470, provided what now is 28 U.S.C. §1331. *Id.* Consequently, even without *federal rights* enforceable under §1983, petitioners can nonetheless challenge state or local action for ongoing violations of *federal law* under federal-question jurisdiction and *Young*.

1. The county respondents lack sovereign immunity.

Counties lack sovereign immunity but can—in some instances—be immune under the arm-of-the-state doctrine. *Compare Alden v. Maine*, 527 U.S. 706, 756-57 (1999) with *Northern Ins. Co. v. Chatham Cty.*,

⁸ Indeed, even if the Secretary had not raised immunity in the district court, he could raise it for the first time here: ““Eleventh Amendment defense sufficiently partakes of the nature of a jurisdictional bar so that it need not be raised in the trial court.” *Edelman v. Jordan*, 415 U.S. 651, 678 (1974).

547 U.S. 189, 193-95 (2006). The counties are not arms of the state here, but even if they were, county officers would remain subject to suit because immunity does not protect ongoing violations of federal law. *See* Section I.E.2, *infra*. In either event, Maricopa officials lack immunity.

2. Sovereign immunity does not protect ongoing violations of federal law.

Petitioners allege that the respondents violated—and continue to violate—the Due Process Clause, which is an ongoing violation of federal law that the Eleventh Amendment does not immunize under the officer-suit exception to sovereign immunity. *Ex parte Young*, 209 U.S. 123, 159-61 (1908). Significantly, “the inquiry into whether suit lies under *Ex parte Young* does not include an analysis of the merits of the claim.” *Verizon*, 535 U.S. at 638. Consequently, there is no further threshold inquiry into the merits of petitioners’ claims at this stage for alleged violations of *federal* law.

Where a complaint alleges violations of *state* law, by contrast, the *Ex parte Young* doctrine does not apply. *Pennhurst State Sch. & Hosp. v. Halderman*, 465 U.S. 89, 106 (1984). For violations of *state election law*, however, *Pennhurst’s* exception to *Ex parte Young’s* exception itself has several exceptions that allow suit.

a. State election law is enforceable under the Elections Clause.

Under *Moore*, “federal courts must not abandon their own duty to exercise judicial review” when non-legislative actors violate state election law. *Moore*, 143 S.Ct. at 2089-90. Compliance with state election law has an enforceable federal component.

b. State election law is enforceable under §1988(a).

In federal civil rights actions, federal law applies “so far as such laws are suitable to carry the same into effect,” but can be supplemented by “the common law, as modified and changed by the constitution and statutes of the State” if “not inconsistent with the Constitution and laws of the United States.” 42 U.S.C. §1988(a).⁹ Although 28 U.S.C. §1343(4) and 42 U.S.C. §1988(a) do not elevate state law to an independent federal cause of action, *Moor v. County of Alameda*, 411 U.S. 693, 700-04 (1973), they do allow federal courts to look to state law as part of resolving federal claims.

c. State election law informs what “process” is “due” regarding the fundamental right to vote.

Generally, the Due Process Clause—and not state law—answers the constitutional question of what process is due. *Cleveland Bd. of Educ. v. Loudermill*, 470 U.S. 532, 541 (1985). In the unique situation of election law, state law can inform the answer to that question not only under 42 U.S.C. §1988(a) but also under the Elections and Electors Clauses, which put the issue of election law for federal purposes in the hands of state Legislatures. Moreover, while it need not rise to a constitutional question, petitioners can sue county officials under state law, without regard to the *Pennhurst* problem that might apply to suing state officials under state law. 28 U.S.C. §1367. For these

⁹ As used in §1988(a), “Title 24” includes 28 U.S.C. §1343 and 42 U.S.C. §1983. *Lynch v. Household Fin. Corp.*, 405 U.S. 538, 544 n.7 (1972).

related reasons, Arizona election law can inform the Court's analysis of the issues presented here.¹⁰

II. THIS COURT SHOULD SUMMARILY REVERSE, BOTH ON THE ORIGINAL RECORD AND A *FORTIORI* ON THE NEW EVIDENCE UNDER §1653.

Summary reversal would be appropriate here for several reasons.

First, the lower courts' rejection of petitioners' pleadings and evidence was inappropriate for an Article III dismissal.

Second, the basis for the lower courts' decision—*Lance*, App:7a—has become unmoored in the lower courts from its actual holding in this Court, which summary resolution could set right.

Third, with major new decisions like *Moore*, the Court can grant, vacate, and remand (“GVR”) for the lower courts to apply the new precedent. *Lawrence v. Chater*, 516 U.S. 163, 166 (1996).

Fourth, and relatedly, the Court occasionally uses follow-on summary decisions to flesh out issues in recently decided cases. *See, e.g., Lambrix v. Singletary*, 520 U.S. 518, 538-39 (1997); Richard C. Chen, *Summary Dispositions as Precedent*, 61 WM. & MARY L. REV. 691, 694 (2020).

Fifth, exigency may justify summary resolution. *United States v. Fortner*, 455 F.3d 752, 754 (7th Cir. 2006). Although easier when an issue presented for

¹⁰ As candidates for state office in 2022, the Elections and Electors Clauses did not apply directly to petitioners' elections, but Arizona state courts would apply the constitutional-doubt canon to read statutes narrowly to avoid readings that cast doubt on a statute's constitutionality. *State v. Arevalo*, 249 Ariz. 370, 373 P 9 (2020).

summary disposition is purely legal, “the Court has not shied away from summarily deciding fact-intensive cases where, as here, lower courts have egregiously misapplied settled law.” *Wearry v. Cain*, 577 U.S. 385, 394-95 (2016) (collecting cases).

A. It is urgent to resolve these issues before the 2024 election.

Two urgent issues must be resolved before the 2024 election.

First, this Court should summarily confine *Lance* to its holding (namely, plaintiffs with nothing at stake except noncompliance with the law suffer only a generalized grievance). That clarity is needed to prevent *Lance* posing an obstacle to voters’ asserting claims under the Elections and Electors Clauses. *See* Section I.A.5.b, *supra*.

Second, the weakness in voting infrastructure requires resolution before the 2024 election. *See* Section III, *supra*. Without resolution, election results in the numerous states with Dominion voting machines—at the very least—cannot be trusted.

B. The district-court record supports summary reversal.

Petitioners’ complaint sufficiently alleged both past injury and risk of future injury, which the lower courts should have accepted for purposes of standing. *Warth v. Seldin*, 422 U.S. 490, 500 (1975); *City of Waukesha v. EPA*, 320 F.3d 228, 235 (D.C. Cir. 2003) (“court ... must ... assume that on the merits the plaintiffs would be successful in their claims”) (citing *Warth*); *Ariz. State Legis. v. Ariz. Indep. Redistricting Comm’n*, 576 U.S. 787, 800 (2015) (distinguishing a court’s perception of a weak merits case from a lack of standing) (citing *Warth*). “Whether a plaintiff has a

legally protected interest (and thus standing) does not depend on whether he can demonstrate that he will succeed on the merits.” *Tyler v. Cuomo*, 236 F.3d 1124, 1133 (9th Cir. 2000). Otherwise, every losing plaintiff would lose for lack of standing.

C. New allegations under §1653 *a fortiori* support summary reversal.

Although the lower courts erred in failing to credit petitioners’ pleadings and evidence at the motion-to-dismiss phase, petitioners’ new evidence, allowable on appeal under 28 U.S.C. §1653—shows not only that the same problems occurred in past elections, but also that the respondents falsely claimed safeguards that would minimize the risk of harm. Both allegations—past harm and lack of safeguards—are allegations of jurisdiction allowable under §1653, Section I.A.1.a, *supra*, and they both alter the Article III analysis of imminence. *See also* Section I.A.2, *supra* (procedural injuries lower Article III’s threshold for imminence). Assuming *arguendo* that the lower courts did not err on the original record, they clearly erred when measured under petitioners’ amended allegations of standing on appeal.

**III. THE QUESTIONS PRESENTED ARE
CRUCIAL TO ENSURING ELECTORAL
INTEGRITY.**

In addition to the “cert-worthy” issues presented here, the election context is urgently important for this Court to resolve in advance of the 2024 election and beyond. Without this Court’s concerted effort, the technical capacity to thwart the will of the electorate will escape detection and meaningful review due to election litigation’s short timeframes and complex civil litigation’s long duration. The fulsome record and

judicially noticeable other materials make this case an ideal vehicle to consider these issues.

A. The fundamental right to vote is “preservative of all rights,” and only this Court can secure that right.

“[T]he political franchise of voting ... is regarded as a fundamental political right, because preservative of all rights.” *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886). As Madison explained, “[t]he qualifications of electors and elected [are] fundamental articles in a Republican [Government] and ought to be fixed by the Constitution,” and “[i]f the Legislature could regulate those of either, it can by degrees subvert the Constitution.” *Oregon v. Mitchell*, 400 U.S. 112, 210 (1970) (quoting 2 M. Farrand, RECORDS OF THE FEDERAL CONVENTION OF 1787, at 249-50 (1911)) (Harlan, J., concurring in part and dissenting in part). While this case concerns only Arizona, petitioners’ new evidence extends to the approximately 30 States that use Dominion systems. This judiciary is the only branch of government that can resolve this matter. If the results of elections in approximately 30 States are unreliable, the political branches’ *lawful* composition circa January 3, 2025, is unknowable.

B. The Court should commit to taking up cases alleging electoral improprieties.

Given the preeminence of voting in our system, this Court should ensure that election cases are not improvidently dismissed under Article III. Often, cases erroneously dismissed will become moot before dismissal can be reversed. That prospect is especially problematic with election litigation, which has a short timeline and often cannot be undone, even when erroneous. Options include affording “special

solicitude” to standing in voting-rights cases, *cf. Massachusetts*, 549 U.S. at 520, and recognizing that cases like this raise procedural or structural claims lowering Article III’s thresholds for immediacy and redressability. *See* Section I.A.2, *supra*. Alternatively, as with racially tainted juries, the Court could commit to hearing election cases beyond the Court’s normal criteria. *See Rose v. Mitchell*, 443 U.S. 545, 556-57 (1979). Without the Court’s commitment to these issues, the threat of electoral misconduct is simply too great.

CONCLUSION

The petition for a writ of *certiorari* should be granted.

March 14, 2024

Respectfully submitted,

KURT B. OLSEN
Olsen Law PC
1250 Connecticut Ave NW
Suite 700
Washington, DC 20036
202-408-7025
ko@olsenlawpc.com

LAWRENCE J. JOSEPH
Counsel of Record
1250 Connecticut Ave NW
Suite 700
Washington, DC 20036
202-355-9452
ljoseph@larryjoseph.com

Counsel for Petitioners

APPENDIX

Lake v. Fontes, No. 22-16413 (9th Cir. Oct. 16, 2023) 1a

Lake v. Hobbs, No. 2:22-cv-0677-JJT (D. Ariz. Aug. 26, 2022) 10a

U.S. CONST. art. I, § 4..... 40a

U.S. CONST. art. II, § 1, cl. 2 40a

U.S. CONST. amend. XI..... 40a

U.S. CONST. amend. XIV, §1 40a

28 U.S.C. §1653 40a

42 U.S.C. §1988(a)..... 41a

A.R.S. §16-442 41a

A.R.S. §16-449 44a

A.R.S. §16-452 45a

A.R.S. §16-1004 46a

A.R.S. §16-1009 47a

A.R.S. §16-1010 47a

Amended Compl. (May 4, 2022)..... 48a

Declaration of Walter C. Daugherty (June 8, 2022) 113a

Declaration of Benjamin R. Cotton (June 8, 2022) 130a

Hearing Transcript (July 21, 2022) (excerpt)..... 144a

**UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

KARI LAKE; MARK FINCHEM,
Plaintiffs-Appellants,

v.

ADRIAN FONTES, Arizona Secretary of State; BILL GATES, as a member of the Maricopa County Board of Supervisors; CLINT HICKMAN, as a member of the Maricopa County Board of Supervisors; JACK SELLERS, as a member of the Maricopa County Board of Supervisors; THOMAS GALVIN, as a member of the Maricopa County Board of Supervisors; STEVE GALLARDO, as a member of the Maricopa County Board of Supervisors; MARICOPA COUNTY BOARD OF SUPERVISORS; REX SCOTT, as a member of the Pima County Board of Supervisors; MATT HEINZ, as a member of the Pima County Board of Supervisors; SHARON BRONSON, as a member of the Pima County Board of Supervisors; STEVE CHRISTY, as a member of the Pima County Board of Supervisors; ADELITA GRIJALVA, as a member of the Pima County Board of Supervisors,

Defendants-Appellees.

No. 22-16413

D.C. No. 2:22-
cv-00677-JJT

OPINION

2a

Appeal from the United States District Court
for the District of Arizona
John Joseph Tuchi, District Judge, Presiding

Argued and Submitted September 12, 2023
Phoenix, Arizona

Filed October 16, 2023

Before: Ronald M. Gould, Andrew D. Hurwitz, and
Patrick J. Bumatay, Circuit Judges.

Per Curiam Opinion

OPINION

PER CURIAM:

Kari Lake and Mark Finchem ("Plaintiffs"), the Republican nominees for Governor and Secretary of State of Arizona, filed this action before the 2022 general election, contending that Arizona's use of electronic tabulation systems violated the federal Constitution.¹ The district court dismissed their operative first amended complaint for lack of Article III standing. *Lake v. Hobbs*, 623 F. Supp. 3d 1015, 1027-29 (D. Ariz. 2022).

Plaintiffs' candidacies failed at the polls, and their various attempts to overturn the election out-

¹ Plaintiffs raised no federal statutory claims and have withdrawn the state law claims raised in their operative complaint on appeal.

come in state court have to date been unavailing.² On appeal, they no longer seek any relief concerning the 2022 election, but instead seek to bar use of electronic tabulation systems in future Arizona elections. We agree with the district court that Plaintiffs' "speculative allegations that voting machines may be hackable are insufficient to establish an injury in fact under Article III," *Lake*, 623 F. Supp. 3d at 1029, and affirm.

I.

Arizona authorized electronic tabulation of election ballots in 1966. *See* H.B. 204, 27th Leg., 2d. Reg. Sess. (Ariz. 1966).³ Under the Arizona election system, voters mark their choices on paper ballots, which are then fed into electronic machines for tabulation. Ariz. Rev. Stat. §§ 16-462, 16-468(2), 16-502(A).⁴ Before being certified for use in elections,

² *See, e.g., Lake v. Hobbs*, 525 P.3d 664 (Ariz. Ct. App. 2023); Order, *Finchem v. Fontes*, No. CV 23-0064, 2023 Ariz. Super. LEXIS 8.

³ Like the district court, we take judicial notice of relevant Arizona statutes and the Secretary of State's 2019 Election Procedures Manual. *See* Fed. R. Evid. 201(b); *Lake*, 623 F. Supp. 3d at 1023 n.5. We find it unnecessary to rely on any testimony from the preliminary injunction hearing. *See id.* at 1023 (citing testimony from preliminary injunction hearing).

⁴ Despite the state-law requirement that voters mark paper ballots, the operative complaint requested that the district court mandate use of "paper ballots" in the 2022 general election. Plaintiffs' attorneys were sanctioned in part for "misrepresentations about Arizona's use of paper ballots." *Lake v. Hobbs*, 643 F. Supp. 3d 989, 1001, 2022 U.S. Dist. LEXIS 216879, *22-23 (D. Ariz. 2022). Appeals of that sanctions order are pending separately. *See Lake v. Gates, et. al.*, No. 23-16022 (9th Cir. *appeal docketed* Jul. 24, 2023); *Lake v. Gates, et. al.*, No. 23-16023 (9th Cir. *appeal docketed* Jul. 24, 2023).

the tabulation machines are tested by an accredited laboratory and the Secretary of State's Certification Committee. Ariz. Rev. Stat. § 16-442; *see also* §16-552 (identical testing requirement for tabulation of early ballots). The certified machines are then subjected to pre-election logic and accuracy tests by the Secretary of State and the election officials of each county. Ariz. Rev. Stat. § 16-449; Ariz. Sec'y of State, 2019 Election Procedures Manual ("2019 EPM") at 86.⁵

After tabulation by machines, the paper ballots cast by each voter are retained for post-election audits and possible recounts. After an election, political party representatives conduct a sample hand count of the paper ballots under the oversight of county elections departments. Ariz. Rev. Stat. § 16-602. The counties then perform additional logic and accuracy testing. 2019 EPM at 235. Arizona law mandates a recount whenever the margin between the top two candidates "is less than or equal to one-half of one percent of the number of votes cast for both such candidates or on such measures or proposals." Ariz. Rev. Stat. § 16-661.

When not in use, the hardware components of electronic tabulation systems are inventoried, stored in secure locations, and sealed with tamper-resistant seals. 2019 EPM at 95-96. An electronic tabulation system may not be connected to the internet, wireless communications devices, or external networks and may "not contain remote access software or any capability to remotely-access the system." 2019 EPM at 96.

⁵ The current manual does not differ from the 2019 Manual in any respect relevant to this opinion. *See* Ariz. Sec'y of State, 2023 Election Procedures Manual.

II.

The gravamen of Plaintiffs' operative complaint is that notwithstanding safeguards, electronic tabulation systems are particularly susceptible to hacking by non-governmental actors who intend to influence election results. Although the operative complaint cites opinions by purported experts on manipulation risk and alleges that difficulties have occurred in other states using electronic tabulation systems, it does not contend that any electronic tabulation machine in Arizona has ever been hacked. And, on appeal, counsel for Plaintiffs conceded that their arguments were limited to potential future hacking, and not based on any past harm.

A.

The district court held that, even accepting the factual allegations of the operative complaint as true, Plaintiffs had not established Article III standing to sue. *Lake*, 623 F. Supp. 3d at 1029. Article III requires, at an "irreducible constitutional minimum," that a plaintiff have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338, 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016) (citing *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560-61, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992)). The plaintiff must demonstrate a "concrete and particularized" and "actual or imminent" "invasion of a legally protected interest." *Lujan*, 504 U.S. at 560. A "concrete" injury must be "real," *Spokeo*, 578 U.S. at 340, and an "imminent" one must be "certainly impending," *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 409, 133 S. Ct. 1138, 185 L. Ed. 2d 264

(2013). "[A]n abstract, theoretical concern will not do." *Pierce v. Ducey*, 965 F.3d 1085, 1089 (9th Cir. 2020).

An injury is "particularized" when it impacts a plaintiff in a "personal and individual way." *Spokeo*, 578 U.S. at 339 (quoting *Lujan*, 504 U.S. at 560 n.1). "An interest shared generally with the public at large in the proper application of the Constitution and laws will not do." *Arizonans for Off. Eng. v. Arizona*, 520 U.S. 43, 64, 117 S. Ct. 1055, 137 L. Ed. 2d 170 (1997); *see also Pierce*, 965 F.3d at 1089.

1.

Plaintiffs assert standing as the nominated candidates of their party and as voters. Because Lake and Finchem are no longer nominated candidates for state office and no longer seek relief related to the 2022 election, they likely now lack standing on that ground. *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2208, 210 L. Ed. 2d 568 (2021) ("Plaintiffs must maintain their personal interest in the dispute at all stages of litigation."). But even assuming Plaintiffs can continue to claim standing as prospective voters in future elections, they have not established the kind of injury Article III requires.

We note as an initial matter that the precise nature of Plaintiffs' claimed injury is not clear. Although Plaintiffs contend that the use of electronic tabulation systems denies them a "fundamental right" to vote, they do not allege that the State has in any way burdened their individual exercise of the franchise. *See, e.g., Harper v. Virginia State Bd. of Elections*, 383 U.S. 663, 665-66, 86 S. Ct. 1079, 16 L. Ed. 2d 169 (1966) (finding a fee an unconstitutional burden on the right to vote). Nor do they claim that

the Arizona system discriminates against them because of race, sex, inability to pay a poll tax, or age. *See* U.S. Const. amends. XV, XIX, XXIV, or XXVI.

Moreover, Plaintiffs do not appear to allege a particularized injury. They do not allege that the tabulation of *their* votes will be manipulated. Rather, as the district court noted, they at most assert a "generalized interest in seeing that the law is obeyed," an interest that "is neither concrete nor particularized." *Lake*, 623 F. Supp. 3d at 1028 (cleaned up); *see also Lance v. Coffman*, 549 U.S. 437, 441-42, 127 S. Ct. 1194, 167 L. Ed. 2d 29 (2007) (finding no particularized injury in voters' challenge to districting plan where "only injury" alleged was that law "has not been followed.").

And, to the extent that Plaintiffs assert a constitutional right to a certain level of accuracy in the Arizona tabulation system, their claim plainly fails.⁶ "[I]t is the job of democratically elected representatives to weigh the pros and cons of various balloting systems," recognizing that "[n]o balloting system is perfect." *Weber v. Shelley*, 347 F.3d 1101, 1106-07 (9th Cir. 2003). Indeed, "the possibility of electoral fraud can never be *completely* eliminated." *Id.* at 1106.

2.

In any event, the district court correctly held

⁶ Plaintiffs cite the "Cyber Ninjas" hand-count audit of Maricopa County votes in 2020 authorized by the Arizona Senate. But, they overlook the audit report's conclusion that "there were no substantial differences between the hand count of the ballots provided and the official election canvass results for Maricopa County." *Maricopa County Forensic Election Audit, Volume I*, at 1 (Sept. 24, 2021), <https://perma.cc/B4EA-U683>.

that Plaintiffs, who claim no past injury, failed to establish that a future injury was either imminent or substantially likely to occur. "Where there is no actual harm . . . its imminence (though not its precise extent) must be established." *Lujan*, 504 U.S. at 564 n.2. Article III requires a "certainly impending" injury or, at the very least, a "substantial risk that the harm will occur," *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158, 134 S. Ct. 2334, 189 L. Ed. 2d 246 (2014) (cleaned up).

Plaintiffs simply have not plausibly alleged a "real and immediate threat of" future injury. *City of Los Angeles v. Lyons*, 461 U.S. 95, 103, 103 S. Ct. 1660, 75 L. Ed. 2d 675 (1983). Rather, as the district court noted, they posit only "conjectural allegations of potential injuries." *Lake*, 623 F. Supp. 3d at 1032. Their operative complaint relies on a "long chain of hypothetical contingencies" that have never occurred in Arizona and "must take place for any harm to occur—(1) the specific voting equipment used in Arizona must have 'security failures' that allow a malicious actor to manipulate vote totals; (2) such an actor must actually manipulate an election; (3) Arizona's specific procedural safeguards must fail to detect the manipulation; and (4) the manipulation must change the outcome of the election." *Id.* at 1028. This is the kind of speculation that stretches the concept of imminence "beyond its purpose." *Lujan*, 504 U.S. at 564 n.2. Plaintiffs' "conjectural allegations of potential injuries," *Lake*, 623 F. Supp. 3d at 1032, are insufficient to plead a plausible "real and immediate threat of" election manipulation, *Lyons*, 461 U.S. at 103.

In the end, none of Plaintiffs' allegations supports a plausible inference that their individual votes

in future elections will be adversely affected by the use of electronic tabulation, particularly given the robust safeguards in Arizona law, the use of paper ballots, and the post-tabulation retention of those ballots.⁷ The district court correctly dismissed the operative complaint for lack of Article III standing.⁸

III

The judgment of the district court is **AF-FIRMED**.

⁷ *Curling v. Kemp*, a decision cited by Plaintiffs finding plausible an allegation of a “future hacking event,” 334 F. Supp. 3d 1303, 1316, 1320 (N.D. Ga. 2018), is not to the contrary. The plaintiffs in that case alleged that the electronic system at issue “was *actually* accessed or hacked multiple times.” *Id.* at 1314. And, the electronic machines used in Georgia did “not create a paper trail.” *Id.* at 1308. In Arizona, “every vote cast can be tied to a paper ballot.” *Lake*, 623 F. Supp. 3d at 1028 n.13.

⁸ We therefore find it unnecessary to address the district court’s holding that the complaint must also be dismissed under the Eleventh Amendment for failure to plausibly allege a constitutional violation. *See Lake*, 623 F. Supp. 3d at 1032.

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

KARI LAKE, *et al.*,
Plaintiffs,

v.

KATIE HOBBS, *et al.*,
Defendants.

No. CV-22-00677-PHX-
JJT

ORDER

At issue are the following motions:

- 1) 1) Defendants Bill Gates, Clint Hickman, Jack Sellers, Thomas Galvin, and Steve Gallardo’s (hereinafter referred to collectively as “Maricopa County Defendants”) Motion to Dismiss (Doc. 27), joined by Sharon Bronson, Steve Christy, Adelita Grijalva, Matt Heinx, and Rex Scott (hereinafter referred to collectively as “Pima County Defendants”) (Doc. 31) and Arizona Secretary of State, Katie Hobbs (“the Secretary”) (Doc. 45), to which Plaintiffs Kari Lake and Mark Finchem responded (Doc. 56), and the Maricopa County Defendants replied (Doc. 61);
- 2) The Maricopa County Defendants’ Motion for Judicial Notice of Exhibits 1 through 17 (Doc. 29), joined by the Pima County Defendants (Doc. 31), to which Plaintiffs responded (Doc. 55);
- 3) The Secretary’s Motion to Dismiss (Doc. 45), to which Plaintiffs responded (Doc. 58), and the Secretary replied (Doc. 62);
- 4) Plaintiffs’ Motion for Preliminary Injunction (Doc. 50), to which the Maricopa County Defendants and the Secretary responded (Docs. 57, 59, respectively), joined by the Pima County Defendants (Doc. 60), and Plaintiffs replied

- (Docs. 64, 63, respectively);
- 5) The Secretary's Motion to Strike and Motion in Limine (Doc. 74), joined by the Maricopa County Defendants (Doc. 75), to which Plaintiffs responded (Doc. 91); and
 - 6) Plaintiffs' Expedited Request for Permission to Supplement Record (Doc. 93), to which Defendant Maricopa County responded (Doc. 95), joined by the Secretary (Doc. 96).

On July 21, 2022, the Court heard the parties' arguments on Defendants' Motions to Dismiss and Plaintiffs' Motion for Preliminary Injunction. (*See* Doc. 79; Doc. 98, Tr.) For the reasons set forth below, the Court grants Defendants' Motions to Dismiss, and therefore does not reach Plaintiffs' Motion for Preliminary Injunction.¹ The Court also denies

¹ To obtain a preliminary injunction, a plaintiff must show that "(1) [it] is likely to succeed on the merits, (2) [it] is likely to suffer irreparable harm in the absence of preliminary relief, (3) the balance of equities tips in [its] favor, and (4) an injunction is in the public interest." *Garcia v. Google, Inc.*, 786 F.3d 733, 740 (9th Cir. 2015) (citing *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 20, 129 S. Ct. 365, 172 L. Ed. 2d 249 (2008)). Plaintiffs cannot meet any of the factors. Further, even if Plaintiffs could satisfy the first, second, and third *Winter* factors, which they cannot, their Motion for Preliminary Injunction would undoubtedly fail on the fourth factor—such an injunction is not in the public interest. Not only do Plaintiffs fail to produce any evidence that a full hand count would be more accurate, but a hand count would also require Maricopa County to hire 25,000 temporary staff and find two million square feet of space. (Tr. 196:6-198:8.) Further, there is no question that the results of the election would be delayed. (Tr. 198:9-21; 199:22-201:14.) In fact, with the County's current employees it would be "an impossibility" to have the ballots counted in order to perform the canvass by the 20th day after the election, as required by

Plaintiffs' Expedited Request for Permission to Supplement Record.

I. BACKGROUND

A. Plaintiffs' Allegations

Plaintiffs allege that the United States' transition to electronic systems and computer technology for voting has "created unjustified new risks of hacking, election tampering, and electronic voting fraud." (Doc. 3, First Amended Complaint ("FAC") ¶ 71.) According to Plaintiffs, electronic ballot marking devices certified by Arizona are "potentially insecure, 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." (FAC ¶ 23.) It follows, Plaintiffs say, that the use of these devices in the upcoming 2022 midterm election, "without objective validation, violates the voting rights of every Arizonan." (FAC ¶ 23.)

Plaintiffs assert that the electronic voting systems used in Arizona counties are "rife" with cybersecurity vulnerabilities and provide a means for unauthorized persons to manipulate the reported vote counts in an election and potentially change the winner. (FAC ¶¶ 12, 139.) Some of the vulnerabilities Plaintiffs identify include: operating systems and antivirus software that lack necessary updates; open ports on the election management server, which allow for possible remote access; shared accounts and common passwords; unauthorized user internet or cellular access through election servers and devices;

law. (Tr. 194:16-23.) Thus, the injunctive relief Plaintiffs seek is not in the public interest.

and secret content not subject to objective and public analysis. (FAC ¶ 12.)

Plaintiffs contend that credible allegations of electronic voting machine glitches that materially impacted specific races began to emerge in 2002. (FAC ¶ 73.) Plaintiffs cite cyber experts and computer scientists who claim that they have created programs and software that can change votes without detection. (FAC ¶¶ 74-75.) Plaintiffs also note that electronic voting machine manufacturers “source and assemble their components in hostile nations,” specifically naming China, Taiwan, and the Philippines. (FAC ¶¶ 90-92.)

According to Plaintiffs, both Republican and Democratic lawmakers have been aware of the problems with electronic voting systems for years but have failed to act. (FAC ¶¶ 93-107.) Further, Plaintiffs claim that electronic voting machine companies have not been transparent about their systems, specifically noting that the Department of Homeland Security’s Cybersecurity and Infrastructure Agency (“CISA”) revealed that “malicious hackers had compromised and exploited SolarWinds Orion network management software products.” (FAC ¶¶ 108-112 (citing CISA, *CISA Issues Emergency Directive to Mitigate the Compromise of SolarWinds Orion Network Management Products* (Dec. 13, 2020) (<https://www.cisa.gov/news/2020/12/13/cisa-issues-emergency-directive-mitigate-compromise-solarwinds-orion-network>)).) Plaintiffs claim that open-source technology would mitigate some of these problems and promote both security and transparency, but Defendants have failed to institute such technologies. (FAC ¶¶ 117-118.) Instead,

according to Plaintiffs, the lack of transparency has created a “black box” system of voting that lacks credibility and integrity. (FAC ¶ 124.)

Plaintiffs also allege that they have found evidence of illegal vote manipulation during the 2020 general election. (FAC ¶ 125.) Plaintiffs cite a report compiled by the Cyber Ninjas, which they claim found that: (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. *Maricopa County Forensic Election Audit, Volume I* at 1-3 (Sept. 24, 2021), https://c692f527-da75-4c86-b5d1-8b3d5d4d5b43.filesusr.com/ugd/2f3470_a91b5cd3655445b498f9acc63db35afd.pdf.²

Next, Plaintiffs contend that Arizona’s voting systems do not meet state or federal standards. (FAC ¶ 135 (citing 2002 Voting Systems Standards

² Plaintiffs fail to mention that the report also states:
[T]here were no substantial differences between the hand count of the ballots provided and the official election canvass results for Maricopa County. This is an important finding because the paper ballots are the best evidence of voter intent and there is no reliable evidence that the paper ballots were altered to any material degree.

Maricopa County Forensic Election Audit, Volume I at 1-3.

(“VSS”); A.R.S. § 16-442(B)).) The Secretary has statutory duties to test, certify, and qualify the software used on county election systems, and Plaintiffs allege she certified Dominion’s DVS 5.5-B voting system despite the fact that it includes Dominion ImageCast Precent2 (“ICP2”), a component program, which does not meet 2002 VSS standards or Arizona’s statutory requirements. (FAC ¶ 137.) By seeking to use the DVS 5.5-B system, Plaintiffs assert that the Secretary intends to facilitate violations of Arizona and federal law, and that such a system cannot ensure that elections are “free and equal” as required by Article 2, Section 21 of the Arizona Constitution. (FAC ¶¶ 142-143.)

Plaintiffs also claim that Arizona’s post-election audit process is insufficient to remediate the security problems inherent in the use of electronic voting machines, because they can be defeated by sophisticated manipulation of the voting machines. (FAC ¶¶ 144-145.) According to Plaintiffs, the only way to overcome the security issues they identify is for the Court to Order that the upcoming midterm election must be conducted by paper ballot. (FAC ¶ 153.) Plaintiffs summarize the procedures they ask the Court to implement as follows:

- 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.

- Th[r]ough 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.

(FAC ¶ 153.) Plaintiffs maintain that the Cyber Ninjas’ hand count “offers Defendant Hobbs a proof-of-concept and a superior alternative to relying on corruptible voting systems,” and that voting jurisdictions outside the U.S., including France and Taiwan, have shown that “hand-count voting can deliver swift, secure, and accurate election results.”³ (FAC ¶ 155.)

B. Elections in Arizona

Before discussing the legal merits of Plaintiffs’ claims, the Court provides a brief overview of Arizona’s current practices surrounding elections. Arizona authorized the use of electronic voting systems in 1966 and has been using them to tabulate votes for decades. H.B. 204, 27th Leg., 2d. Reg. Sess. (Ariz. 1966).

³ When asked how long the Cyber Ninjas’ hand count took to complete, Douglas Logan, one of Plaintiffs’ witnesses, testified that “there was more than just hand counting, but we started hand counting in the middle of April and we finished with the delivery of the report . . . September 22.” (Tr. 79:1-9.) “[T]he majority of [the hand count] was done in about two and a half or three months, but there was a lot of quality control work we did to make sure those numbers were accurate.” (Tr. 73:21-24.) During the hand count, roughly 2,000 individuals worked to hand count only two races. (Tr. 72:12-22.)

Before a single vote is cast, Arizona's election equipment undergoes thorough testing by independent, neutral experts. Electronic voting equipment must be tested by both the Secretary's Certification Committee and an Election Assistance Commission ("EAC")⁴ accredited testing laboratory before it may be used in an Arizona election. A.R.S. § 16-442(A), (B). Before the 2020 election, for example, Maricopa County's Dominion Voting Systems Democracy Suite 5.5-B equipment underwent testing by Pro V&V, an EAC-accredited testing laboratory, and received a Certificate of Conformance from the EAC. (Doc. 29, Exs. 2, 3, 4⁵.) In October 2019, the Arizona Secretary of State's Equipment Certification Committee also conducted a demonstration of the equipment in a public meeting, which the equipment

⁴ The EAC was established by the Help America Vote Act of 2002, which charged the Commission with providing "for the testing, certification, decertification, and recertification of voting system hardware and software by accredited laboratories." 52 U.S.C. § 20971(a)(1).

⁵ The County Defendants filed a Motion for Judicial Notice of Exhibits 1-17 to their Motion to Dismiss. (Doc. 29.) The Court grants the Motion only as to the government documents referenced in this Order. The remainder of the Motion is denied. The Court also acknowledges that in their memorandum in opposition to Defendants' Motion, Plaintiffs argue that judicial notice is inappropriate where Defendants seek to use government documents "willy-nilly to 'prove' disputed facts." (Doc. 55 at 1.) The Court disagrees with Plaintiffs' argument. The facts contained in the documents cited by the Court in this Order are not subject to reasonable dispute. Fed. R. Evid. 201(b)(2). For the same reasons, the Court takes judicial notice of the portions of government websites cited by both parties. Further, the Court notes that it only refers to these facts for the purpose of providing background for its later analysis, not to establish the truth of any disputed fact.

also passed. (Doc. 29, Ex. 5.)

In addition to the equipment certification process, Arizona’s vote tabulation results are subject to four independent audits—two audits occur before the election, and two audits after. The first of these audits is a logic and accuracy test, which is performed by the Arizona Secretary of State on a sample of the tabulation equipment. A.R.S. § 16-449(A), (B). As Scott Jarrett (“Mr. Jarrett”), Maricopa County’s Director of Elections, explained during the July 21, 2022 hearing, even before the Secretary of State performs her logic and accuracy testing, the County tests the equipment.⁶ During Maricopa County’s logic and accuracy tests for the 2020 general election, over 8,100 ballots were tested to ensure that every candidate, every rotational position, and every ballot style would be counted accurately. (Tr. 188:12-16.) The Secretary’s logic and accuracy tests are blind to the County, and are observed by representatives from the political parties, who sign off on the results. (Tr. 188:19-189:4.) On October 6, 2020, prior to the 2020 election, the Secretary of State performed the logic and accuracy testing on Maricopa County’s tabulation equipment, and the ballots were tabulated with 100% accuracy. (Doc. 29, Ex. 9; *see also* Maricopa Cnty., *Maricopa County Election Facts | Voting*

⁶ Mr. Jarrett also explained that Maricopa County performs a “hash code verification” prior to the Secretary’s logic and accuracy testing. (Tr. 187:15-24.) As the Court understands it, a unique hash code value provides a digital representation of every piece of equipment and software that should be installed on the Election Management System, and the County does a one-for-one check to ensure that no erroneous or malicious software or hardware has been added to the equipment.

Equipment & Accuracy (last accessed Aug. 17, 2022), <https://www.maricopa.gov/5539/Voting-Equipment-Facts> (hereinafter “Maricopa Cnty. Election Facts”.) The second required audit also takes place before election day. For the second audit, Arizona counties must perform a logic and accuracy test on all of their tabulation equipment. 2019 Elections Procedures Manual (“2019 EPM”) at 86. In 2020, the second Maricopa County audit also took place on October 6, and the tabulators counted the ballots with 100% accuracy. (Maricopa Cnty. Election Facts.)

When the time to vote arrives, every Arizona voter casts a ballot by hand, on paper. This is the law. See A.R.S. §§ 16-462 (primary election ballots “shall be printed”), 16-468(2) (“Ballots shall be printed in plain clear type in black ink, and for a general election, on clear white materials”), 16-502 (general election ballots “shall be printed with black ink on white paper”). Arizona’s statutes carve out one exception to this rule—voters with disabilities may vote on “accessible voting devices” (sometimes referred to as “ballot marking devices,” or “BMDs”), but these devices still must produce a paper ballot or voter verifiable paper audit trail, which the voter can review to confirm that the machine correctly marked his or her choices, and which can be used in the event of an audit.⁷ A.R.S. §§ 16-442.01; § 16-

⁷ In *Curling v. Raffensperger*, the plaintiffs’ expert, Professor J. Alex Halderman, noted in his report that “Georgia can eliminate or greatly mitigate [the risks of electronic ballot marking devices (“BMDs”)] 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.” (Halderman Dec. 33, Doc. 1304-3, *Curling v.*

446(B)(7); 2019 EPM at 80. As Mr. Jarrett explained, the accessible voting devices are not connected to the internet, and the ports on the devices are locked and have affixed tamper evident seals.⁸ (Tr. 177:5-20.) There has never been an instance where one of the seals was removed or broken during voting. (Tr. 178:4-9.) The Secretary also certifies the accessible voting systems for each county. *See* Ariz. Sec’y of State, *Voting Equipment* (last accessed Aug. 17, 2022), <https://azsos.gov/elections/voting-election/voting-equipment>. In the 2020 general election, 2,089,563 ballots were cast in Maricopa County, and only 453 of those were cast using an accessible voting device. (Tr. 174:24-175:4.)

Following the election, the third required audit—a hand count—takes place.⁹ A.R.S. § 16-602(B).

Raffensperger, No. 1:17-CV-2989-AT (N.D. Ga. Feb. 3. 2022) (emphasis added)). This is already Arizona’s practice.

⁸ Mr. Jarrett testified that serialized port blockers with customized keys are also used on Maricopa County’s vote tabulation equipment. (Tr. 178:19-179:7.) The equipment is also enclosed in security containers, which prevent access to all ports, even those that may have a mouse or a keyboard plugged in. (Tr. 179:8-15.) The keys to the security containers are locked in a secure server room, to which only three people have access, and upon entering the secure server room, those three individuals must keep a log of their reasons for doing so. (Tr. at 179:15-20.)

⁹ This audit can only be performed if the county chairs of each political party designate and provide election board members to conduct the hand count. (Doc. 27 at 5, fn. 4; A.R.S. § 16-602(B)(7).) One or more of the political party chairs in Apache, Gila, Graham, La Paz, and Yuma did not designate election board members for the 2020 general election, so hand count audits were not performed in those counties. (Doc. 27 at 5, fn. 4; *see also* Ariz. Sec’y of State, *Summary of Hand Count*

Representatives of the political parties, under the oversight of the Elections Department, randomly select two percent of the polling locations, as well as one percent of the early ballots cast or five thousand early ballots, whichever is less, and count all the ballots by hand. A.R.S. §§ 16-602(B), (F); EPM at 215. Maricopa County's hand count audit of the 2020 general election was conducted from November 4 through 9, 2020, and showed that the tabulators had counted the ballots with 100% accuracy. (Doc. 29, Ex. 10.)

The fourth required audit is the post-election logic and accuracy testing performed by the counties. Each county performs its own post-election logic and accuracy testing. EPM at 235. This process uses the same test ballots as the counties' pre-election logic and accuracy testing, and should generate the same results, verifying that no changes were made to the tabulators' software between the two tests. EPM at 235. Maricopa County's post-election logic and accuracy testing took place on November 18, 2020, and showed that the tabulators counted the votes with 100% accuracy. (Doc. 29, Ex. 11; see also Maricopa Cnty., Media Advisory: Post Election Logic and Accuracy Test on Nov. 18 (Nov. 17, 2020) <https://content.govdelivery.com/accounts/AZMARIC/bulletins/2acfff>; Maricopa Cnty., Board of Supervisors Certifies Maricopa County Election Results (Nov. 20, 2020) <https://content.govdelivery.com/accounts/AZMARIC/bulletins/2ada05e>.)

In February 2021, Pro V&V and SLI Compliance,

Audits - 2020 General Election (Nov. 17, 2020), <https://azsos.gov/2020-general-election-hand-count-results>.)

another EAC-accredited laboratory, conducted audits of Maricopa County's tabulation equipment. (Doc. 27, Ex. 6.) The two auditors reached the same conclusions: (1) all systems and equipment were using software and equipment certified by the EAC and Arizona Secretary of State; (2) no malicious hardware or software discrepancies were detected; (3) the system was determined to be a "closed network" and no internet connections were identified; and (4) logic and accuracy testing resulted in accurate numbers.¹⁰

C. Procedural History

Plaintiffs brought this action under 42 U.S.C. § 1983 and *Ex parte Young*, 209 U.S. 123, 28 S. Ct. 441, 52 L. Ed. 714 (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. (FAC ¶ 48.) Specifically, Plaintiffs allege that the Secretary has violated A.R.S. §§ 16-452 (A), (B), and (D); 16-446 (B); 16-445(D); and § 16-442(B).¹¹ (FAC ¶¶ 156-161.) They also allege that the County Defendants have

¹⁰ Logic and accuracy testing was outside SLI Compliance's scope of work, so was performed only by Pro V&V. (Doc. 29, Ex. 6 at 1.)

¹¹ During the July 21, 2022 hearing, Plaintiffs took the position that the FAC does not present claims that are based in state law, and they "are not alleging [Defendants' actions] violate[] state statute[s]." (Tr. 224:12-225:3.) However, paragraphs 177, 184, 190, 196, and 207 are clear: in bringing their claims under federal law, "Plaintiffs incorporate and reallege all paragraphs in this Complaint." This includes paragraphs 156-161, where Plaintiffs allege the Secretary acted in violation of Arizona state law.

violated A.R.S. §§ 11-251¹² and 16-452 (A). (FAC ¶¶ 162-165.) Plaintiffs further allege that all Defendants have violated the Due Process Clause of the Fourteenth Amendment of the U.S. Constitution and Article 2, Section 4 of the Arizona Constitution; the Equal Protection Clause of the Fourteenth Amendment; and the fundamental right to vote as protected by the U.S. Constitution. (*See generally* FAC.) They seek declaratory and injunctive relief against all Defendants pursuant to 42 U.S.C. § 1983, as well as a declaratory judgment pursuant to 28 U.S.C. § 2201. (FAC ¶¶ 196-199, 207-211.)

The County Defendants filed a Motion to Dismiss Plaintiffs' claims under Federal Rule of Civil Procedure 12(b)(6), arguing that (1) Plaintiffs' claims are untimely; (2) Plaintiffs fail to allege sufficient factual allegations; and (3) Plaintiffs fail to allege a cognizable legal theory. (*See generally* Doc. 27.) The Secretary joined in the County Defendants' arguments, and also filed her own Motion to Dismiss under Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), arguing that (1) Plaintiffs lack standing; (2) the Eleventh Amendment bars Plaintiffs' claims; and (3) Plaintiffs fail to state a cognizable constitutional claim. (*See generally* Doc. 45.)

On July 21, 2022, the Court heard the parties' arguments on Plaintiff's Motion for Preliminary Injunction and Defendants' Motions to Dismiss. In this Order, the Court addresses only the Defendants' arguments concerning standing, the Eleventh Amendment, and portions of Defendants' arguments that pertain to the timing of Plaintiffs' suit, because

¹² Plaintiffs are no longer pursuing their A.R.S. § 11-251 claim. (Doc. 27 at 19.)

it finds that each of these arguments is dispositive on its own.

II. LEGAL STANDARDS

A. Federal Rule of Civil Procedure 12(b)(1)

“A motion to dismiss for lack of subject matter jurisdiction under Rule 12(b)(1) may attack either the allegations of the complaint as insufficient to confer upon the court subject matter jurisdiction, or the existence of subject matter jurisdiction in fact.” *Renteria v. United States*, 452 F. Supp. 2d 910, 919 (D. Ariz. 2006) (citing *Thornhill Publ’g Co. v. Gen. Tel. & Elecs. Corp.*, 594 F.2d 730, 733 (9th Cir. 1979)). “Where the jurisdictional issue is separable from the merits of the case, the [court] may consider the evidence presented with respect to the jurisdictional issue and rule on that issue, resolving factual disputes if necessary.” *Thornhill*, 594 F.2d at 733; *see also Autery v. United States*, 424 F.3d 944, 956 (9th Cir. 2005) (“With a 12(b)(1) motion, a court may weigh the evidence to determine whether it has jurisdiction.”). The burden of proof is on the party asserting jurisdiction to show that the court has subject matter jurisdiction. *See Indus. Tectonics, Inc. v. Aero Alloy*, 912 F.2d 1090, 1092 (9th Cir. 1990).

B. Article III Standing

Article III Courts are limited to deciding “cases” and “controversies.” U.S. Const. art. III, § 2. “Article III of the Constitution requires that one have “the core component of standing.” *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992). To have standing under Article III, a plaintiff must show: (1) an injury in fact that is (a) concrete and particularized and (b) actual or imminent; (2) the injury is fairly traceable to the challenged action of the defendant; (3) it is likely, not

merely speculative, that the injury will be redressed by decision in the plaintiff's favor. *Maya v. Centex Corp.*, 658 F.3d 1060, 1067 (9th Cir. 2011). A complaint that fails to allege facts sufficient to establish standing requires dismissal for lack of subject-matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1). *See, e.g., Chandler v. State Farm Mut. Auto. Ins. Co.*, 598 F.3d 1115, 1123 (9th Cir. 2010).

C. The Eleventh Amendment

The Eleventh Amendment prevents a state from being sued in federal court without its consent. *Seven Up Pete Venture v. Schweitzer*, 523 F.3d 948, 952 (9th Cir. 2008). When the state is “the real, substantial party in interest,” Eleventh Amendment immunity extends to “suit[s] against state officials.” *Pennhurst State Sch. & Hosp. v. Halderman*, 465 U.S. 89, 101, 104 S. Ct. 900, 79 L. Ed. 2d 67 (1984) (quotations omitted). *Ex parte Young* provides an exception to Eleventh Amendment immunity, but it applies only to “claims seeking prospective injunctive relief against state officials to remedy a state’s ongoing violation of federal law.” *Ariz. Students’ Ass’n v. Ariz. Bd. of Regents*, 824 F.3d 858, 865 (9th Cir. 2016) (citing *Ex parte Young*, 209 U.S. 123, 28 S. Ct. 441, 52 L. Ed. 714 (1908)).

D. The Purcell Doctrine

The *Purcell* doctrine directs federal appellate courts “to weigh, in addition to the harms attendant upon issuance or nonissuance of an injunction, considerations specific to election cases and its own institutional procedures.” *Purcell v. Gonzalez*, 549 U.S. 1, 4, 127 S. Ct. 5, 166 L. Ed. 2d 1 (2006). The Supreme Court “has repeatedly emphasized that lower federal courts should ordinarily not alter the

election rules on the eve of an election.” *Republican Nat’l Comm. v. Democratic Nat’l Comm.*, 140 S. Ct. 1205, 1207, 206 L. Ed. 2d 452 (2020) (collecting cases); *Short v. Brown*, 893 F.3d 671, 676 (9th Cir. 2018) (“[T]he Supreme Court has warned us many times to tread carefully where preliminary relief would disrupt a state voting system on the eve of an election.”); *see also New Georgia Project v. Raffensperger*, 976 F.3d 1278, 1283 (11th Cir. 2020) (“And we are not on the eve of the election—we are in the middle of it, with absentee ballots already printed and mailed.”).

III. ANALYSIS

A. Plaintiffs Lack Article III Standing

To establish an injury in fact, the first element of standing, “a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical.” *Spokeo, Inc. v. Robins*, 578 U.S. 330, 339, 136 S. Ct. 1540, 194 L. Ed. 2d 635 (2016) (quotations omitted). A “concrete” and “particularized” injury must be “real,” not “abstract,” *id.*, and “must affect the plaintiff in a personal and individual way.” *Raines v. Byrd*, 521 U.S. 811, 819, 117 S. Ct. 2312, 138 L. Ed. 2d 849 (1997) (quotation omitted). And to be “actual or imminent,” a threatened injury must be “certainly impending”— “allegations of possible future injury are not sufficient.” *Clapper v. Amnesty Int’l USA*, 568 U.S. 398, 409, 133 S. Ct. 1138, 185 L. Ed. 2d 264 (2013) (cleaned up).

The Secretary argues that Plaintiffs cannot establish an injury in fact for two reasons. First, the Secretary argues that Plaintiffs’ claimed injuries are too speculative to establish standing. (Doc. 45 at 5.)

According to the Secretary, the bulk of Plaintiff's allegations are vague, and have to do with electronic voting systems generally. (Doc. 45 at 6.) She also notes that all of Plaintiffs' examples of "issues" with election equipment involve other jurisdictions, not Arizona. (Doc. 45 at 6; *see also* FAC ¶¶ 4, 23, 29, 32, 61, 73-80, 81-89, 90-92, 93-102, 103-106, 107, 108-116, 125-131, 133-134, 181, 199.) The Secretary cites *Shelby Cnty. Advocs. for Valid Elections v. Hargett* to support her position. 2019 U.S. Dist. LEXIS 156740, 2019 WL 4394754 (W.D. Tenn. Sept. 13, 2019), *aff'd* *Shelby Advocs. for Valid Elections v. Hargett*, 947 F.3d 977 (6th Cir. 2020). There, the district court found that the plaintiffs' allegations that their county's electronic voting equipment was "vulnerable to undetectable hacking and malicious manipulation" were "based only on speculation, conjecture and [the plaintiffs'] seemingly sincere desire for their 'own value preferences' in having voting machines with a paper trail." 2019 U.S. Dist. LEXIS 156740, [WL] at *2, 7. The district court held that the plaintiffs had failed to allege facts to show that "Shelby County's voting system is more likely to miscount votes than any other system used in Tennessee," and the allegations in their complaint were therefore too conjectural to survive. 2019 U.S. Dist. LEXIS 156740, [WL] at 10.

Plaintiffs argue that "[a]n allegation of future injury may suffice if . . . there is a substantial risk that the harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158, 134 S. Ct. 2334, 189 L. Ed. 2d 246 (2014) (quotation omitted). They point to their Complaint for support, contending that it "pleads detailed allegations showing that existing safety procedures and certifications can be defeated

and that manipulation of votes can be performed without leaving any record of the changes.” (Doc. 58 at 4; FAC ¶¶ 31, 75, 98, 128, 138-40, 145-46.) Plaintiffs also cite *Curling v. Kemp*, where the U.S. District Court for the Northern District of Georgia held that the plaintiffs had standing where they “plausibly allege[d] a threat of a future hacking event that would jeopardize their votes and the voting system at large.” *Curling v. Kemp*, 334 F. Supp. 3d 1303, 1316 (N.D. Ga. 2018).

Ultimately, even upon drawing all reasonable inferences in Plaintiffs’ favor, the Court finds that their claimed injuries are indeed too speculative to establish an injury in fact, and therefore standing. This case is nothing like *Curling v. Kemp*. There, the plaintiffs alleged that specific voting machines used in Georgia had actually been accessed or hacked multiple times, and despite being notified about the problem repeatedly, Georgia officials failed to take action. *Curling v. Kemp*, 334 F. Supp. 3d at 1314-1317. Here, as the Secretary points out, a long chain of hypothetical contingencies must take place for any harm to occur— (1) the specific voting equipment used in Arizona must have “security failures” that allow a malicious actor to manipulate vote totals; (2) such an actor must actually manipulate an election; (3) Arizona’s specific procedural safeguards must fail to detect the manipulation; and (4) the manipulation must change the outcome of the election. (See Doc. 62 at 2-3.) Plaintiffs fail to plausibly show that Arizona’s voting equipment even has such security failures.¹³ And even if the allegations in Plaintiff’s

¹³ Defendants have taken numerous steps to ensure such security failures do not exist or occur in Arizona or Maricopa

complaint were plausible, their alleged injury is not “certainly impending” as required by *Clapper*. 568 U.S. at 409.¹⁴

Second, the Secretary argues that Plaintiffs cannot establish an injury in fact because they fail to show that their alleged injury is particularized. (Doc. 45 at 8.) The Secretary again cites *Shelby Cnty. Advocs. for Valid Elections* to assert that Plaintiffs’ claims represent a “general dissatisfaction with the voting system and processes” used in Arizona. 2019 U.S. Dist. LEXIS 156740, 2019 WL 4394754, at *9. While it is well-established that a generalized “interest in seeing that the law is obeyed” is neither concrete nor particularized, Plaintiffs allege, and the Secretary does not consider, whether Plaintiffs’ status as candidates may confer standing. *See, e.g., Pierce v. Ducey*, 965 F.3d 1085, 1089 (9th Cir. 2020).

During the July 21 hearing, Plaintiffs argued “[a]nytime ... the playing field in an election is tilted in any way, standing is -- exists for the candidates.” (Tr. 244:8-9.) It is true that, as candidates, Plaintiffs “have a cognizable interest in ensuring that the final vote tally accurately reflects the legally valid votes cast. An inaccurate vote tally is a concrete and

County. As the Court chronicled in painstaking detail in Section I.B, every vote cast can be tied to a paper ballot (*see* A.R.S. §§ 16-442.01; § 16-446(B)(7); 2019 EPM at 80), voting devices are not connected to the Internet (*see* Doc. 29, Ex. 6) any ports are blocked with tamper evident seals (*see* Tr. 177:5-20), and access to voting equipment is limited (*see* Tr. at 179:15-20).

¹⁴ As set forth in Section I.B, Defendants have extensive post-election audit procedures in place to detect and reconcile any problems with tabulation machine counts if an intrusion did occur.

particularized injury to candidates.” *Carson v. Simon*, 978 F.3d 1051, 1058 (footnote omitted); *Trump v. Wis. Elections Comm’n*, 983 F.3d 919, 924 (7th Cir. 2020). However, while Plaintiffs’ status as candidates does make the argument that their alleged injuries are particularized more compelling, it is not sufficient to establish standing. Simply put, Plaintiffs have not alleged facts to show that it is plausible that the field is “tilted” here. *See Stein v. Cortés*, 223 F. Supp. 3d 423, 432-33 (E.D. Pa. 2016) (finding no standing where the plaintiff, an unsuccessful candidate, alleged that Pennsylvania’s DRE electronic voting machines may be susceptible to hacking).

For the foregoing reasons, this Court joins many others that have held that speculative allegations that voting machines may be hackable are insufficient to establish an injury in fact under Article III. *See Stein*, 223 F. Supp. 3d at 432-33; *Samuel v. Virgin Islands Joint Bd. of Elections*, 2013 U.S. Dist. LEXIS 31538, 2013 WL 842946, at *5 (D.V.I. Mar. 7, 2013) (finding no standing on the grounds that the plaintiffs’ “conjectural” allegations “that the election process ‘may have been’ left open to compromise” by using certain voting machines were “amorphous due process claims, without requisite concreteness”); *Schulz v. Kellner*, 2011 U.S. Dist. LEXIS 73088, 2011 WL 2669456, at *7 (N.D.N.Y. July 7, 2011) (allegations that “votes will allegedly not be counted accurately” because of “machine error and human fraud resulting from Defendants’ voting procedures” were “merely conjectural and hypothetical” and insufficient to establish standing); *Landes v. Tartaglione*, 2004 U.S. Dist. LEXIS 22458, 2004 WL 2415074, at *3 (E.D. Pa. Oct. 28, 2004),

aff'd, 153 F. App'x 131 (3d Cir. 2005) (finding no standing because the plaintiff's claim "that voting machines are vulnerable to manipulation or technical failure" was "conjectural or hypothetical").

B. The Eleventh Amendment Bars Plaintiffs' Claims

Even if Plaintiffs had standing, dismissal of their claims is warranted under the Eleventh Amendment. As mentioned *supra*, Plaintiffs bring this action under 42 U.S.C. § 1983 and *Ex parte Young* to challenge government officers' ongoing violation of federal law." (FAC ¶ 48 (citing 209 U.S. 123, 28 S. Ct. 441, 52 L. Ed. 714 (1908)).) However, as the Secretary points out, *Ex parte Young* cannot apply here, because, despite Plaintiffs' claims that their constitutional rights have been violated, Plaintiffs do not plausibly allege a violation of federal law. (Doc. 45 at 9.) To support this argument, the Secretary cites a multitude of cases. For example, in *Weber v. Shelley*, the Ninth Circuit held that "[n]othing in the Constitution" forbade the use of touchscreen voting systems as an alternative to paper ballots, noting that it is "the job of democratically-elected representatives to weigh the pros and cons of various balloting systems." 347 F.3d 1101, 1107 (9th Cir. 2003). Other federal courts have reached similar conclusions. In *Pettengill v. Putnam County R-1 Sch. Dist.*, the Eighth Circuit unequivocally stated that there is no constitutional basis for federal courts to oversee the administrative details of local elections. 472 F.2d 121, 122 (8th Cir. 1973) ("[The] complaint asks the federal court to oversee the administrative details of a local election. We find no constitutional basis for doing so."). The Fourth Circuit has also held that "[a] state may employ diverse methods of voting,

and the methods by which a voter casts his vote may vary throughout the state.” *Hendon v. N.C. State Bd. of Elections*, 710 F.2d 177, 181 (4th Cir. 1983.) Furthermore, in a case similar to the one presently before the Court, the Southern District of New York held that the use of voting machines is “for the elected representatives of the people to decide[.] There is no constitutional right to any particular method of registering and counting votes.” *Green Party of N.Y. v. Weiner*, 216 F. Supp. 2d 176, 190-91 (S.D.N.Y. 2002).¹⁵

Plaintiffs counter that the Secretary’s Eleventh Amendment argument is erroneous, because she argues the Plaintiff’s claims fail on the merits and ignores their constitutional arguments. (Doc. 58 at 9.) According to Plaintiffs, “[t]o be constitutional, election regulations must produce a reliable count of the legal votes. Plaintiffs’ ... allege that Arizona’s equipment and system do not.” (Doc. 58 at 9-10.) Thus, according to Plaintiffs, they allege a violation of federal law. Plaintiffs also attempt to distinguish *Weber*, which the Secretary cites, because the court there reviewed a grant of summary judgment. 347 F.3d at 1105. The Court finds this line of argument unpersuasive.

¹⁵ In any event, insofar as Plaintiffs argue a constitutional violation grounded in Arizona’s failure to require voting by paper ballots, their allegations are flatly wrong. The Court finds for purposes of determining jurisdiction, that as set forth *supra*, 99.98% of voters in Arizona cast their votes by marking and submitting paper ballots in the 2020 election, and the remaining 0.02% —representing mostly sight impaired voters— cast their ballots on system-generated paper ballots which could be verified before casting to ensure they reflected those voters’ choices.

The Eleventh Amendment bars Plaintiffs' claims. Because the Constitution charges states with administering elections, Plaintiffs' claims can only stem from an argument that Defendants are violating state law by using what Plaintiffs allege are insecure or inaccurate voting systems. Plaintiffs argued at the hearing in this matter that their claims do not depend on any application of Arizona state law, and the Court need not determine whether Defendants' procedures comply with state law to grant Plaintiffs relief, but as set forth above, they are incorrect. Indeed, Arizona state laws set forth detailed requirements concerning how ballots are counted and how voting systems are used. *See* A.R.S. §§ 16-400 and 16-411 *et seq.* Absent a constitutional right to a particular method of voting, Plaintiffs' claims that Arizona's voting systems are flawed can *only* arise under state law¹⁶, and such claims are barred. Courts have repeatedly rejected alleged federal constitutional claims that rely on a determination that state officials have not complied with state law. *See S&M Brands, Inc. v. Georgia ex rel. Carr*, 925 F.3d 1198, 1204-05 (11th Cir. 2019); *see also Bowyer v. Ducey*, 506 F.Supp.3d 699, 716 (D. Ariz. 2020) ("where the claims are state law claims, masked as federal law claims" Eleventh Amendment immunity applies). Moreover, the Court fails to see how Plaintiffs' requested relief would not violate the "principles of federalism that underlie the Eleventh Amendment." *Pennhurst State Sch. & Hosp. v.*

¹⁶ In fact, Plaintiffs' First Amended Complaint repeatedly so alleged (FAC ¶¶ 156-161), directly contradicting the position Plaintiffs now take in an attempt to overcome the Eleventh Amendment bar Defendants have raised.

Halderman, 465 U.S. 89, 106, 104 S. Ct. 900, 79 L. Ed. 2d 67 (1984). If the Court were to enjoin Defendants from using electronic voting systems, retain jurisdiction to ensure compliance, and require Defendants to conduct elections according to Plaintiffs’ preferences, the Court would unavoidably become impermissibly “entangled, as [an] overseer[] and micromanager[], in the minutiae of state election processes.” *Ohio Democratic Party v. Husted*, 834 F.3d 620, 622 (6th Cir. 2016).

C. Plaintiffs’ Suit is Untimely

Finally, even if the Court could properly retain jurisdiction over Plaintiff’s claims, it could not grant the injunctive relief Plaintiffs request. The 2022 Midterm Elections are set to take place on November 8. In the meantime, Plaintiffs request a complete overhaul of Arizona’s election procedures.

In advancing their *Purcell* argument, the County Defendants emphasize the strain on elections officials that would be prompted by such a late change to elections procedures. (Doc. 27 at 9.) During the July 21 hearing, Mr. Jarrett testified that Maricopa County “could not” switch to precinct-based polling locations, as Plaintiffs request, before the November election. (Tr. 198:14-21.) Mr. Jarrett also testified that thousands more workers would be needed for a full hand count, and Maricopa County already struggles to retain enough poll workers. (Tr. 198:2-8, 199:22-200:5.) For example, for the August primary, Maricopa County had to increase its wages from \$14 to \$19 per hour, and still fell “woefully short” of the number of workers it needed for the primary. (Tr. 198:2-6.)

The County Defendants also cite a number of

cases from this election cycle where federal courts have invoked *Purcell* to deny requests for injunctive relief. The Court finds *League of Women Voters of Fla., Inc. v. Fla. Sec’y of State* instructive. 32 F.4th 1363, 1371 (11th Cir. 2022). In that case, the district court granted an injunction when voting was set to begin in less than four months, but the Eleventh Circuit stayed the district court’s injunction pending appeal. *Id.* The Eleventh Circuit based its reasoning on Justice Kavanaugh’s concurrence in *Merrill v. Milligan*, U.S. , 142 S. Ct. 879, 880, L.Ed.2d (2022), holding that under *Purcell*, the standard a plaintiff must meet to obtain “injunctive relief that will upset a state’s interest in running its elections without judicial interference” is heightened. *Id.* at 1372. This means that the plaintiff “must demonstrate, among other things, that its position on the merits is ‘entirely clearcut’” in order for a district court to grant injunctive relief. *Id.* Here, Plaintiffs filed their Motion for Preliminary Injunction on June 15, 2022 (Doc. 50), and on July 21, 2022, soon after the motion was fully briefed the Court held a hearing. At the time of the hearing, the November election was already less than four months away. Further, as the Court has suggested throughout this Order, Plaintiffs’ position is a far cry from “entirely clearcut.”

Plaintiffs argue that *Purcell* does not apply on these facts, because it stands for the “principle that a federal court should not cause confusion among voters by enjoining state election laws immediately before an election.” (Doc. 56 at 8 (citing 549 U.S. at 4-5).) Here, according to Plaintiffs, the election was not imminent when they brought this action. *See, e.g., Ariz. Democratic Party v. Hobbs*, 976 F.3d 1081,

1086-87 (9th Cir. 2020). Plaintiffs also argue that here, voters will be “entirely unaffected” by the injunctive relief they seek, because the relief “applies only after a ballot is submitted.” *Self Advocacy Sol. N.D. v. Jaeger*, 464 F. Supp. 3d 1039, 1055 (D.N.D. 2020) (internal quotations omitted). Instead, Plaintiffs assert, *Purcell* weighs in favor of granting injunctive relief, because they seek to “vindicate” *Purcell*’s concern for the “integrity of our electoral processes.” (Doc. 56 at 10 (citing 549 U.S. at 4).)

The Court finds Plaintiffs’ reading of *Purcell* unconvincing. In applying *Purcell*, Courts have made clear that it stands for more than just the proposition that federal courts should avoid changes in law that may cause voter confusion. The County Defendants are correct to assert that courts applying *Purcell* also “caution federal courts to refrain from enjoining election law too close in time to an election if the changes will create administrative burdens for election officials.” (Doc. 61 at 5.) *See Ariz. Democratic Party*, 976 F.3d at 1086 (“And, as we rapidly approach the election, the public interest is well served by preserving Arizona’s existing election laws, rather than by sending the State scrambling to implement and to administer a new procedure for curing unsigned ballots at the eleventh hour.”) The injunctive relief Plaintiffs seek would not just be challenging for Arizona’s election officials to implement; it likely would be impossible under the extant time constraints.

IV. CONCLUSION

For the foregoing reasons, Plaintiffs’ First Amended Complaint is dismissed in its entirety. While the Court agrees with Plaintiffs that the right to vote is precious, and should be protected, Plaintiffs

lack standing because they have articulated only conjectural allegations of potential injuries that are in any event barred by the Eleventh Amendment, and seek relief that the Court cannot grant under the *Purcell* principle.

IT IS THEREFORE ORDERED granting Defendants' Motions to Dismiss (Docs. 27, 45), and granting in part the County Defendants' Motion for Judicial Notice (Doc. 29).

IT IS FURTHER ORDERED denying as moot Plaintiffs' Motion for Preliminary Injunction (Doc. 50) and Defendants' Motion to Strike (Doc. 74).

IT IS FURTHER ORDERED denying Plaintiffs' Expedited Motion to Supplement Record (Doc. 93).¹⁷

¹⁷ In their Expedited Motion (Doc. 93), Plaintiffs request to supplement the record with evidence they argue would either undermine or impeach the testimony of Mr. Jarrett as to the security of Maricopa County's electronic ballot counting equipment. The request is extraordinarily and inexcusably untimely, and in any event does not remedy the speculative nature of Plaintiffs' claims. Plaintiffs initiated this action according to their preference. The Court set the hearing by an Order issued well in advance, and Plaintiffs had ample time to prepare their evidence. At the hearing, Mr. Jarrett's testimony was consistent with, if not identical to, his prior appearance before the Arizona Senate and his other statements detailing Maricopa County's election system security and verification procedures, so Plaintiffs had ample notice of what he was going to say at the hearing here. Nonetheless, Plaintiffs waited nearly two weeks after the hearing to ask to submit another declaration, in what appears to be an effort to get the last word and cast doubt on Mr. Jarrett's testimony at a point when the County could no longer respond. The Court will not allow such potential gamesmanship; nor will it, in the alternative, allow the submission and then a response from Defendants. Such a step would breed satellite litigation and deprive the Court of

39a

IT IS FURTHER ORDERED directing the Clerk of Court to enter judgment accordingly and close this case.

Dated this 26th day of August, 2022.

/s/ John J. Tuchi

Honorable John J. Tuchi

United States District

the ability to evaluate witnesses and their credibility live at hearing.

U.S. CONST. art. I, § 4

The times, places and manner of holding elections for Senators and Representatives, shall be prescribed in each state by the legislature thereof; but the Congress may at any time by law make or alter such regulations, except as to the places of choosing Senators.

U.S. CONST. art. II, § 1, cl. 2

Each state shall appoint, in such manner as the Legislature thereof may direct, a number of electors, equal to the whole number of Senators and Representatives to which the State may be entitled in the Congress[.]

U.S. CONST. amend. XI

The judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by citizens of another state, or by citizens or subjects of any foreign state.

U.S. CONST. amend. XIV, §1

All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

28 U.S.C. §1653

Defective allegations of jurisdiction may be amended, upon terms, in the trial or appellate courts.

42 U.S.C. §1988(a)

The jurisdiction in civil and criminal matters conferred on the district courts by the provisions of titles 13, 24, and 70 of the Revised Statutes for the protection of all persons in the United States in their civil rights, and for their vindication, shall be exercised and enforced in conformity with the laws of the United States, so far as such laws are suitable to carry the same into effect; but in all cases where they are not adapted to the object, or are deficient in the provisions necessary to furnish suitable remedies and punish offenses against law, the common law, as modified and changed by the constitution and statutes of the State wherein the court having jurisdiction of such civil or criminal cause is held, so far as the same is not inconsistent with the Constitution and laws of the United States, shall be extended to and govern the said courts in the trial and disposition of the cause, and, if it is of a criminal nature, in the infliction of punishment on the party found guilty.

A.R.S. §16-442

A. The secretary of state shall appoint a committee of three persons, to consist of a member of the engineering college at one of the universities, a member of the state bar of Arizona and one person familiar with voting processes in the state, no more than two of whom shall be of the same political party, and at least one of whom shall have at least five years of experience with and shall be able to render an opinion based on knowledge of, training in or education in electronic voting systems, procedures and security. The committee shall investigate and test the various types of vote recording or tabulating machines or devices that may be used under this

article. The committee shall submit its recommendations to the secretary of state who shall make final adoption of the type or types, make or makes, model or models to be certified for use in this state. The committee shall serve without compensation.

B. Machines or devices used at any election for federal, state or county offices may only be certified for use in this state and may only be used in this state if they comply with the help America vote act of 2002 and if those machines or devices have been tested and approved by a laboratory that is accredited pursuant to the help America vote act of 2002.

C. After consultation with the committee prescribed by subsection A of this section, the secretary of state shall adopt standards that specify the criteria for loss of certification for equipment that was used at any election for federal, state or county offices and that was previously certified for use in this state. On loss of certification, machines or devices used at any election may not be used for any election for federal, state or county offices in this state unless recertified for use in this state.

D. The secretary of state may revoke the certification of any voting system or device for use in a federal, state or county election in this state or may prohibit for up to five years the purchase, lease or use of any voting system or device leased, installed or used by a person or firm in connection with a federal, state or county election in this state, or both, if either of the following occurs:

1. The person or firm installs, uses or permits the use of a voting system or device that is not certified

for use or approved for experimental use in this state pursuant to this section.

2. The person or firm uses or includes hardware, firmware or software in a version that is not certified for use or approved for experimental use pursuant to this section in a certified voting system or device.

E. The governing body of a city or town or the board of directors of an agricultural improvement district may adopt for use in elections any kind of electronic voting system or vote tabulating device approved by the secretary of state, and thereupon the voting or marking device and vote tabulating equipment may be used at any or all elections for voting, recording and counting votes cast at an election.

F. The secretary of state or the governing body may provide for the experimental use of a voting system or device without a final adoption of the voting system or device, and its use at the election is as valid as if the machines had been permanently adopted.

G. After consultation with the committee prescribed by subsection A of this section, the secretary of state may approve for emergency use an upgrade or modification to a voting system or device that is certified for use in this state if the governing body establishes in an open meeting that the election cannot be conducted without the emergency certification. Any emergency certification shall be limited to no more than six months. At the conclusion of the certification period the voting system or device shall be decertified and unavailable for future use unless certified in accordance with this section.

A.R.S. §16-449

A. Within the period of time before the election day prescribed by the secretary of state in the instructions and procedures manual adopted pursuant to section 16-452, the board of supervisors or other election officer in charge, or for an election involving state or federal candidates, the secretary of state, shall have the automatic tabulating equipment and programs tested to ascertain that the equipment and programs will correctly count the votes cast for all offices and on all measures. Public notice of the time and place of the test shall be given at least forty-eight hours prior thereto by publication once in one or more daily or weekly newspapers published in the town, city or village using such equipment, if a newspaper is published therein, otherwise in a newspaper of general circulation therein. The test shall be observed by at least two election inspectors, who shall not be of the same political party, and shall be open to representatives of the political parties, candidates, the press and the public. The test shall be conducted by processing a preaudited group of ballots so marked as to record a predetermined number of valid votes for each candidate and on each measure and shall include for each office one or more ballots that have votes in excess of the number allowed by law in order to test the ability of the automatic tabulating equipment and programs to reject such votes. If any error is detected, the cause therefor shall be ascertained and corrected and an errorless count shall be made before the automatic tabulating equipment and programs are approved. A copy of a revised program shall be filed with the secretary of state within forty-eight hours after the revision is made. If the error was created by automatic tabulating equipment malfunction, a

report shall be filed with the secretary of state within forty-eight hours after the correction is made, stating the cause and the corrective action taken. The test shall be repeated immediately before the start of the official count of the ballots in the same manner as set forth above. After the completion of the count, the programs used and the ballots shall be sealed, retained and disposed of as provided for paper ballots.

B. Electronic ballot tabulating systems shall be tested for logic and accuracy within seven days before their use for early balloting pursuant to the instructions and procedures manual for electronic voting systems that is adopted by the secretary of state as prescribed by section 16-452. The instructions and procedures manual shall include procedures for the handling of ballots, the electronic scanning of ballots and any other matters necessary to ensure the maximum degree of correctness, impartiality and uniformity in the administration of an electronic ballot tabulating system.

C. Notwithstanding subsections A and B of this section, if a county uses accessible voting equipment to mark ballots and that accessible voting equipment does not independently tabulate or tally votes, the secretary of state in cooperation with the county officer in charge of elections may designate a single date to test the logic and accuracy of both the accessible voting equipment and electronic ballot tabulating systems.

A.R.S. §16-452

A. 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. The secretary of state shall also adopt rules regarding fax transmittal of unvoted ballots, ballot requests, voted ballots and other election materials to and from absent uniformed and overseas citizens and shall adopt rules regarding internet receipt of requests for federal postcard applications prescribed by section 16-543.

B. The rules shall be prescribed in an official instructions and procedures manual to be issued not later than December 31 of each odd-numbered year immediately preceding the general election. Before its issuance, the manual shall be approved by the governor and the attorney general. The secretary of state shall submit the manual to the governor and the attorney general not later than October 1 of the year before each general election.

C. A person who violates any rule adopted pursuant to this section is guilty of a class 2 misdemeanor.

D. 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. §16-1004

A. A person who at any election knowingly interferes in any manner with an officer of such election in the discharge of the officer's duty, or who induces an officer of an election or officer whose duty it is to ascertain, announce or declare the result of such election, to violate or refuse to comply with the

officer's duty or any law regulating the election, is guilty of a class 5 felony.

B. A person who knowingly modifies the software, hardware or source code for voting equipment without receiving approval or certification pursuant to section 16-442 is guilty of a class 5 felony.

C. A person who knowingly impersonates any election official, including an election board member or other poll worker or a challenger or party representative designated pursuant to section 16-590, is guilty of a class 6 felony.

A.R.S. §16-1009

A public officer upon whom a duty is imposed by this title, who knowingly fails or refuses to perform that duty in the manner prescribed by law, is guilty of a class 3 misdemeanor.

A.R.S. §16-1010

A person charged with performance of any duty under any law relating to elections who knowingly refuses to perform such duty, or who, in his official capacity, knowingly acts in violation of any provision of such law, is guilty of a class 6 felony unless a different punishment for such act or omission is prescribed by law.

PARKER DANIELS KIBORT
Andrew Parker (028314)
888 Colwell Building
123 Third Street North
Minneapolis, Minnesota 55401
Telephone: (612) 355-4100
Facsimile: (612) 355-4101
parker@parkerdk.com
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 capac-
ity as members of the Mari-
copa County Board of Supervi-
sors; Rex Scott, Matt Heinz,
Sharon Bronson, Steve Christy,
Adelita Grijalva, in their capac-
ity as members of the Pima
County Board of Supervisors,
Defendants.

No. 2:22-cv-00677-
DMF

**AMENDED COM-
PLAINT**

(Jury Trial Demand)

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 ano-

nymity; 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. The Arizona Constitution provides that “[a]ll elections shall be free and equal.” Ariz. Const. art. 2 § 21. Defendant Hobbs, as Arizona Secretary of State and the chief election officer in Arizona, has enabled a process fundamentally at odds with this requirement..

10. Defendant Hobbs violated state and federal law in several respects, including her failure 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.

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

12. 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.

13. Pima County uses election equipment and systems that are in substance and defect the same as the equipment and systems used in Maricopa Coun-

ty. 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.

14. 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”).

15. 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.

16. 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.

17. 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.

18. 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 Elec-

tion.

19. 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

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

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

22. 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.

23. 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.

24. All electronic voting machines and election

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

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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

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

31. 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.

32. 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.

33. 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.

34. 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

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

36. 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.

37. 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.

38. 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.

39. 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.

40. 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.

41. 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.

42. 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).

43. 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.

44. 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, and to prescribe an official instructions and procedures manual before each such election. A.R.S. §§ 16-446, 16-452.

45. 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”).

46. 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”).

47. 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

48. 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.

49. 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.

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

51. 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.

52. 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.

53. This Court has jurisdiction to award nominal and compensatory damages under 28 U.S.C. §

1343(a)(4).

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

55. 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.

56. 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

57. 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 Mid-term Election, without disclosing the systems and subjecting them to neutral, expert analysis.²

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

59. After the recount of the 2000 presidential election in Florida and the ensuing *Bush v. Gore* decision, Congress passed the Help America Vote Act

²

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

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.

60. 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.

61. 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 Michigan, Princeton University, Georgetown University, and other institutions and presented to various con-

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>).

gressional 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 cellular networks, directly or indirectly.

62. 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.

63. 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.

64. 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.

65. 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 tools “build the election project,” and its technology provides “solutions” for “voting & tabulation,” and “tallying & reporting,”

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

and “auditing the election.” The products sold by Dominion include ballot marking machines, tabulation machines, and central tabulation machines, among others.

66. 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.

67. 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.

68. 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.

69. 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 system in order to subject it to neutral expert evaluation.

70. 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

71. 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.

72. 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.

73. 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 failures that include:

- “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

74. 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

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

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>.

75. 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 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.

76. 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."

77. 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

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>).

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.]”

78. 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



79. 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 regis-

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/>).

tration 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

80. After these revelations about the 2016 election, Jake Braun, a former security advisor for the Obama administration and organizer of the DEF-CON Hacking Conference was 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.”

81. 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.

82. The Georgia plaintiffs supported their allega-

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>).

tions 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.

83. Another piece of expert evidence in the Georgia litigation is a declaration from Harri Hursti 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 inade-

quate “hardening” against a security attack.¹¹

84. 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.’”

85. Concerns in Georgia proved to be well-founded. After scanned ballot images were designated as “public records” under Georgia Senate Bill 202, a report made public by VoterGA revealed, among other things, that 17,724 votes in Fulton County were somehow counted and certified through tabulation machines, despite having no corresponding ballot images. The report further concluded that 132,284 mail-in ballot images do not have a .sha signature file, meaning these ballots cannot be authenticated.

86. 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 the internet because they didn’t know

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

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

87. Prior to 2020, ES&S had represented to its customers and potential customers that its DS200 voting system was “fully certified and compliant with EAC guidelines” even if used with a modem—a critical access point by which unauthorized access can be made. In a letter dated March 20, 2020, the U.S. Election Assistance Commission (EAC) issued a letter to ES&S stating that ES&S had misrepresented that its voting machines with modems were EAC compliant. The EAC ordered ES&S to take corrective actions, including to:

- Revise ES&S’s marketing material to properly represent voting systems that have been certified by the EAC.
- Provide the EAC with a plan to removal all misrepresented marketing material from circulation.

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>).

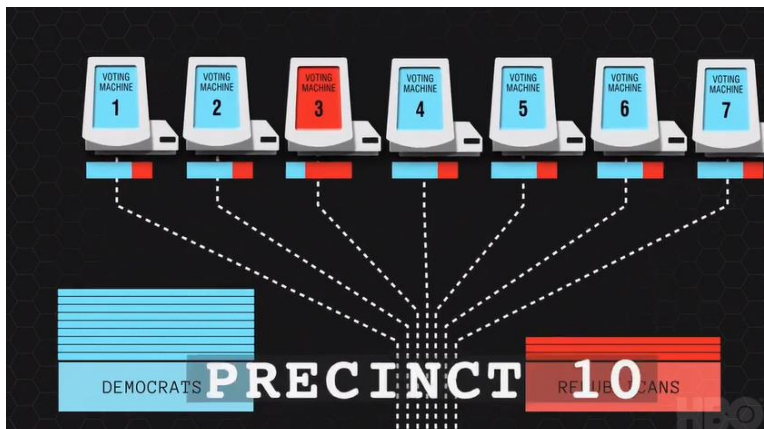
- Notify ES&S's customers and potential customers that previous information was inaccurate.
- Provide customers and potential customers with corrected information.

88. This is not the first time that ES&S has been caught in a lie about the voting machines it sells. In 2018, Vice reported that ES&S falsely denied selling voting machines with remote access software, a fact ES&S later admitted was true in a letter to Senator Ron Wyden (D. Or.).¹⁴

89. 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.¹⁵

¹⁴ Kim Zetter, *Top Voting Machine Vendor Admits It Installed Remote-Access Software on Systems Sold to States*, Vice (July 17, 2018) (<https://www.vice.com/en/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states>).

¹⁵ Screenshot from <https://www.facebook.com/KillChainDoc/videos/2715244992032273/>.



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

90. 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.”¹⁶

91. 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 investigation that affected

¹⁶ CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT at 25 (2018) (<https://homeland.house.gov/imo/media/doc/TFESReport.pdf>).

multiple companies (2015), and a government contractor providing intelligence services (2018).¹⁷

92. Leading electronic voting machine manufacturers source many parts from China, Taiwan, and the Philippines.¹⁸

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

93. 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.

94. 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:¹⁹ “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

¹⁷ 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>).

¹⁸ 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>).

¹⁹ CONGRESSIONAL TASK FORCE ON ELECTION SECURITY, FINAL REPORT (2018) (<https://homeland.house.gov/imo/media/doc/TFESReport.pdf>).

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 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.”²⁰

95. 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.”

96. Senator Wyden did not see his concerns addressed. On December 6, 2019, he, along with his

²⁰ *Id.* at 6-7.

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 skimmed 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 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.[]”

97. 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.”

98. 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.”

99. 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....”

100. 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.”

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

102. 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.²¹

103. 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, Democracy Suite 5.5-A failed the test. On January 24, 2020, the Texas Secretary of State denied certifi-

²¹ PN1758 — Dara Lindenbaum — Federal Election Commission, <https://www.congress.gov/nomination/117th-congress/1758>; https://www.youtube.com/watch?v=wCPLL_D_spc

cation of the system for use in Texas elections.

104. 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."

105. 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."

106. 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.

107. Though Texas did certify ES&S elec-

tronic 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

108. 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.²²

109. 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.

110. 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....”²³ During the 2020 election Dominion election equipment was connected

²² 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>).

²³ 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).

to the internet when it should not have been.²⁴ A Dominion representative in Wayne County, Michigan stated that during the voting in the 2020 election there were irregularities with Dominion’s election equipment, including that equipment was connected to the internet and equipment had scanning issues.

111. 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.²⁵ 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.²⁶

²⁴ Aff. of Patrick J. Colbeck, *Costantino v. City of Detroit*, no. 20-014780-AW (Wayne Co., Mich. Cir. Ct. Nov. 8, 2020).

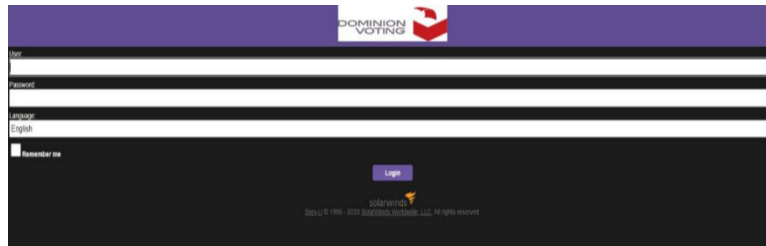
²⁵ Kim Zetter, *Cause of Election Day Glitch in Georgia Counties Still Unexplained*, Politico (Nov. 12, 2020) (<https://www.politico.com/news/2020/11/04/georgia-election-machine-glitch-434065>).

²⁶ 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).

112. 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.²⁷ On April 15, 2021, the White House announced imposition of sanctions on Russia in response to Russian “malicious cyber activities, such as the SolarWinds incident.”²⁸

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

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



115. 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

²⁷ 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>).

²⁸ 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/>).

been hacked, or has malware installed.

116. On November 3, 2021, the Tennessee Secretary of State's office reported to the Election Assistance Commission (EAC) that an "anomaly" was observed during a municipal election in Williamson, County Tennessee, which used Dominion tabulators for a municipal election. This anomaly caused the scanners to mislabel valid ballots as provisional, and therefore did not include these ballots in the poll report totals. After conducting a formal investigation, the EAC concluded the so-called "anomaly" was likely rooted in "erroneous code" present in Dominion's system. How the "erroneous code" came to be on the voting machine, or how such code was not detected in the certification process or other safety testing procedures, was not included in the investigative report.

117. 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.

118. 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.

119. Open source technology fosters transparency, which is why government agencies have employed it for well over a decade. As the U.S. De-

partment of Defense notes on its website, the following policies apply at the federal level to promote the use of open source programs:

- The Federal Source Code Policy, OMB Memo 16-21, establishes policy regarding consideration of acquiring custom-developed code, requiring agencies to consider the value of publishing custom code as OSS, and establishing a OSS Pilot Program to release 20% of all custom-developed code as OSS. The DoD was later directed to implement this program by Section 875 of the National Defense Authorization Act for FY2018.
- The DoD CIO issued a memorandum titled “Clarifying Guidance Regarding Open Source Software (OSS)” on 16 October 2009, which superseded a memo May 2003 memo from John Stenbit.
- The Department of Navy CIO issued a memorandum with guidance on open source software on 5 Jun 2007.
- The Open Technology Development Roadmap was released by the office of the Deputy Under Secretary of Defense for Advanced Systems and Concepts, on 7 Jun 2006.
- The Office of Management and Budget issued a memorandum providing guidance on software acquisition which specifically addressed open source software on 1 Jul 2004.
- US Army Regulation 25-2, paragraph 4-6.h, provides guidance on software security controls that specifically addresses open source software.²⁹

²⁹ Available at <https://dodcio.defense.gov/open-source-software-faq/#q-what-policies-address-the-use-of-open-source-software-oss-in-the-department-of-defense>.

120. In 2016, the Obama administration “introduced a new Federal Source Code Policy that called on every agency to adopt an open source approach, create a source code inventory, and publish at least 20% of written code as open source. The administration also launched Code.gov, giving agencies a place to locate open source solutions that other departments are already using.”³⁰

121. Earlier this year, the San Francisco Board of Supervisors unanimously passed legislation to authorize the use of open source technologies in the Midterm Election.³¹ San Francisco likely would have done this long ago, were it not for Dominion’s obstruction.

122. As reported by the *San Francisco Examiner* in November of last year:

“San Francisco’s Elections Department failed to make progress on developing open-source voting technology for more than a decade, while relying heavily on a voting machine company that sees such technology as a threat to its business interests...

San Francisco Elections Director John Arntz conferred closely with Dominion Voting Systems, once forwarding the company a city report on open-source voting technology before he had read the report himself...

³⁰ Venky Adivi, *The Stars are Aligning for Federal IT Open Source Software Adoption*, TechCrunch (Aug. 27, 2021) (<https://techcrunch.com/2021/08/27/the-stars-are-aligning-for-federal-it-open-source-software-adoption/>).

³¹ Available at https://sanfrancisco.granicus.com/player/clip/40379?view_id=10&redirect=true

Dominion was the only company to bid on Arntz's last contract, in which it doubled its rates to \$12 million spread over the next six years."³²

123. Public functions, like voting, should be open to the public. Certain policymakers outside of Arizona understand and have embraced this principle, while Defendants and voting machine companies have shirked it.

124. This lack of transparency 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

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

126. Dominion Democracy Suite software was used to tabulate votes in 62 Colorado counties, including Mesa County, during the 2020 election. Subsequent examination of equipment from Mesa 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

³² Jeff Elder, *San Francisco Pushes Ahead Towards Open-Source Voting Program*, (Nov. 17, 2021) (<https://www.sfexaminer.com/news/san-francisco-pushes-ahead-towards-open-source-voting-program/>).

County server during Colorado’s November 2020 and April 2021 elections.

127. 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.

128. 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.”

129. 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.³³

³³ M.D. Kittle, *Emails: Green Bay’s ‘Hidden’ Election Networks*, Wisconsin Spotlight (Mar. 21, 2021)

130. In April 2021, the Biden administration announced sanctions against Russia for election interference and hacking in the 2020 United States presidential election.³⁴

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

132. 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.³⁵

133. Retired Wisconsin Supreme Court Justice Michael Gableman conducted an investigation of

(<https://wisconsinspotlight.com/emails-green-bays-hidden-election-networks/>).

³⁴ 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>).

³⁵ *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).

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.”³⁶ 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.”

134. 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.³⁷

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

135. 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).

136. 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 da-

³⁶ Office of the Special Counsel: Second Interim Investigative Report On the Apparatus & Procedures of the Wisconsin Elections System, March 1, 2022, p. 13.

³⁷ Hearing of Georgia Senate Judiciary Subcommittee on Elections, Dec. 30, 2020 (<https://www.youtube.com/watch?v=D5c034r0RIU> beginning at 4:07:58).

ta 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]

137. 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").

138. 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 provides an access point for unauthorized remote connection and thereby makes 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.

139. 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 . . .”

140. 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.

141. 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.

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

143. 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. Such a system cannot ensure that elections in Arizona, including the Midterm Election, are “free and equal,” as required by Article 2, Section 21 of the Arizona Constitution.

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

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

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

146. 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.

147. 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.

148. 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.

149. 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.

150. 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.

151. 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 au-

ditions 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.

152. 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

153. 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.

154. 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.

155. 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

156. 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 rules shall be prescribed in an official instructions and procedures manual to be issued not later than December 31 of each odd-numbered year immediately preceding the general election. Before its issuance, the manual shall be approved by the governor and the attorney general. The

secretary of state shall submit the manual to the governor and the attorney general not later than October 1 of the year before each general election.”

A.R.S. § 16-452 (B).³⁸

- “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).

157. 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).

³⁸ Defendant Hobbs’s failure to timely issue an official instructions and procedures manual is currently the subject of an action brought by Attorney General Brnovich before the Yavapai County Superior Court (case no. P-1300-CV-202200269).

158. 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).

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

160. 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.

161. 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

162. 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.

163. 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).

164. 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.

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

L. Imminent Injury

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

167. 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.

168. 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.

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

170. 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.

171. 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.

172. 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.

173. 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.

174. 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.

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

176. 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)

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

178. 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.

179. 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.

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

- to provide reasonable and adequate protection against the real and substantial threat of electronic and other intrusion and manipula-

tion by individuals and entities without authorization to do so;

- 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;
- to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law; and
- to provide a reasonable and adequate method for voting by which Arizona electors' votes would be accurately counted.

181. 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.

182. 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.

183. 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)

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

185. 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.

186. 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.

187. 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.

188. 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.

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, injunctive relief against these Defendants is warranted.

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

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

191. 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).

192. 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).

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

- 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;
- to ensure that all such equipment, firmware, and software is reliable, accurate, and capable of secure operation as required by law; and
- to provide a reasonable and adequate method for voting by which Arizona electors' votes would be accurately counted.

194. 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.

195. Defendants' violation of the fundamental right to vote 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 Plain-

tiffs, 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)*

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

197. 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.

198. 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.

199. 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)

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

201. 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.

202. 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.

203. 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 to preserve order and to transact business.

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

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

206. Unless Maricopa Defendants and Pima Defendants are enjoined by this Court, then Plaintiffs will have no 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 Maricopa Defendants and Pima Defendants)

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

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

209. The Court has the authority pursuant to 28 U.S.C. § 2201 to issue an Order declaring that it is unconstitutional for the State of Arizona to conduct an election in which the votes are not accurately or securely tabulated.

210. 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.

211. Because of the issues described above regarding the election system to be used by Defendants, the Court should issue an Order declaring that it is unconstitutional for the State to conduct an election which relies on the use of electronic voting systems to cast or tabulate the votes.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

1. Enter an Order 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 153 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. Enter an Order awarding 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: May 4, 2022. **PARKER DANIELS KIBORT**

LLC

By /s/ Andrew D. Parker

Andrew D. Parker (AZ Bar No. 028314)

888 Colwell Building

123 N. Third Street

Minneapolis, MN 55401

Telephone: (612) 355-4100

Facsimile: (612) 355-4101

parker@parkerdk.com

OLSEN LAW, P.C.

By /s/ Kurt Olsen

Kurt Olsen (D.C. Bar No. 445279)*

1250 Connecticut Ave., NW, Suite 700

Washington, DC 20036

Telephone: (202) 408-7025

ko@olsenlawpc.com

* To be admitted *Pro Hac Vice*

*Counsel for Plaintiffs Kari Lake
and Mark Finchem*

112a

By /s/ Alan Dershowitz
Alan Dershowitz (MA Bar No.
121200)*
1575 Massachusetts Avenue
Cambridge, MA 02138

* To be admitted *Pro Hac Vice*

*Of Counsel for Plaintiffs Kari
Lake and Mark Finchem*

**UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA**

Kari Lake, *et al*,

Plaintiffs,

v.

Katie Hobbs, Arizona

Secretary of State, *et al.*,

Defendants.

No. 2:22-cv-00677-JJT

DECLARATION OF WALTER C. DAUGHERITY

WALTER C. DAUGHERITY declares, under penalty of perjury, pursuant to 28 U.S.C. § 1746, that the following is true and correct.

Introduction

1. I am a Senior Lecturer Emeritus in the Department of Computer Science and Engineering at Texas A&M University and also a computer consultant to major national and international firms, as well as to government agencies, including classified work.

2. Prior to my retirement in 2019, I taught computer science and engineering at both the undergraduate and graduate levels for 37 years, the last 32 years being at Texas A&M University. Courses I developed and taught include courses in artificial intelligence, expert systems, programming and software design, quantum computing, and cyberethics.

3. I have published 26 research articles related to expert systems, fuzzy logic, noise-based logic, and quantum computing from over \$2.8 million in funded research projects, plus conference papers and other

publications.

4. As a computer expert I have consulted for major national and international firms, including IBM Federal Systems Division, *New York Times*, *Washington Post*, *Los Angeles Times*, Southwestern Bell Telephone, Fulbright & Jaworski (Houston), and Phonogram B.V. (Amsterdam), and also for government agencies such as Cheyenne and Arapaho Tribes of Oklahoma, Texas Department of Agriculture, U. S. Customs Service, and classified work.

5. Further details about my qualifications are included in my Curriculum Vitae attached as Exhibit A.

6. I analyzed the Cast Vote Records (“CVR”) for numerous counties in the United States, including Pima County and Maricopa County in Arizona. The CVR collects in spreadsheet format the selections contained on each ballot in the order recorded through the tabulator machines without any information that would identify the voter (i.e., no name, address, Social Security number, driver’s license number, voter registration number, etc.).

7. My analysis below of the CVR data shows, in my expert opinion, that in the November 2020 election for which the CVR data was made available, ballots in Maricopa County and Pima County were artificially processed through the tabulators tracking a Proportional-Integral-Derivative (PID) type control function in a closed-loop feedback system. A PID controller or variations of it is a software coded algorithm to maintain a measured process variable (that is, an outcome, such as a ratio) at a pre-specified desired setpoint.

8. PID controllers are used everywhere, from cruise control in automobiles to Category III autoland for an aircraft making a landing when the runway is completely fogged in, to industrial automation of all kinds, such as robots, refineries and other chemical plants, manufacturing quality control, and self-driving cars.

9. An analysis of the actual cumulative ratios of the vote tallies for early mail-in and in-person votes prior to Election Day (“early votes”) for the ten races analyzed in Maricopa County and the seventeen races in Pima County shows a significant and systematic decline in the cumulative ratio as counting progresses. For example, the graph in ¶ 18 below shows the first block of ballots being 75% for a candidate, the next block of ballots being 74% for the candidate, the next block of ballots being 73%, and so on, systematically declining all the way to Election Day.

10. This near straight-line decrease in the cumulative ratio falls within a narrow band for the races analyzed in Maricopa County and in Pima County. Such a uniform and predictable pattern is so statistically implausible that it would not occur without artificial manipulation.

11. As detailed below, my analysis shows to a reasonable degree of scientific and mathematical certainty that vote counting by electronic voting machines used in Maricopa County, Pima County, and other counties throughout the United States that I have examined was manipulated and tightly controlled to reach predetermined outcomes. This manipulation could have been performed manually or by computer, but for reasons described below it is unlikely to have been performed manually.

**Early Vote Counting Was Manipulated In
Pima County, Arizona**

12. In the November 2020 General Election there were numerous contests on the ballot in Pima County, Arizona, from the office of the Presidency down to local county races, and judicial retention questions, propositions, etc.

13. After the election I received the CVR public record report for Pima County, Arizona, from Benny White, one of the candidates for office in Pima County.

14. My analysis of the CVR demonstrates a PID function at work in all 17 races I analyzed.

15. For the November 3, 2020, election 526,319 ballot records are listed in the “2020 General Election Post Election CVR (Cast Vote Record) Aggregate” file, with CVR sequence numbers 1 through 526,332. (Thirteen of those numbers do not appear, confirming that the total number of Cast Vote Records is 526,319, which equals 526,332 minus 13. The materials that I reviewed did not explain why these 13 entries were stricken.)

16. Since the early votes were not sorted and batched by precincts¹ before Election Day as Election Day votes were, by looking to see where in the CVR file consecutive ballots are all from the same precinct we can determine the point at which Election Day

¹ Technically, the “precinct number” 1 to 249 in the CVR file is a *voting district* which is determined by actual precinct, U. S. House district, state Senate district, Board of Supervisors district, school district, etc.; each voting district requires a unique ballot. However, following common usage, we will also call these voting districts “precincts”.

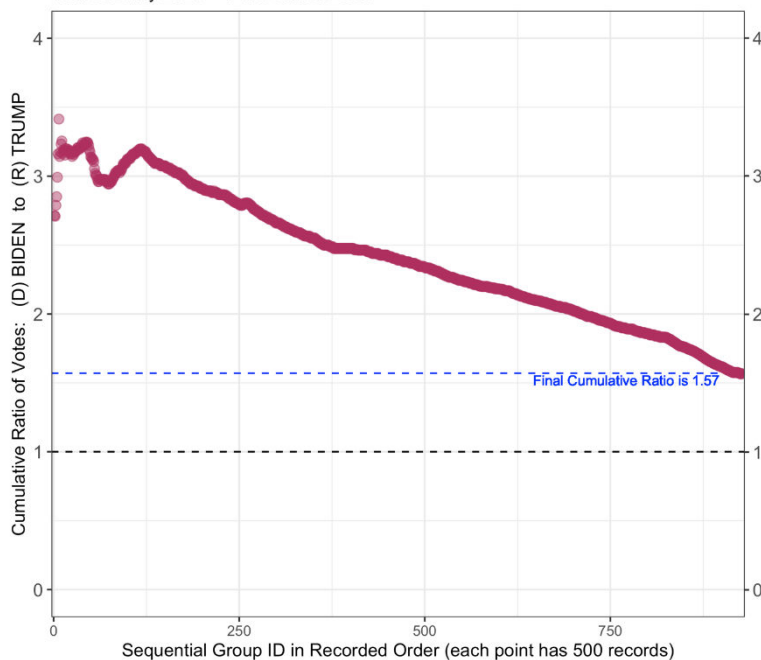
counting began. The first batch of ballots with consecutive precinct numbers starts with CVR# 413,241 for precinct 208, so the early votes are CVR# 1 through 413,239 (since CVR# 413,240 is one of the 13 missing numbers).

17. Graphing the CVR public record report data as the cumulative Democrat/Republican ratio in the data's CVR sequence shows that the CVR entries are not independent of each other or of their order in the CVR, which they should be. In other words, knowing one block of votes was 75% for a candidate should not allow one to predict whether the next block would be a higher or lower percentage, much less to predict that it would be 74% (instead of 63% or 85% or some other value).

18. This manipulated systematic decline is illustrated in the graph² below of this ratio in the Presidential race:

² All graphs were prepared at my direction by Cynthia Butler, a professional statistician.

Cumulative Ratio of Votes: (D) BIDEN -to- (R) TRUMP
 Contest: PRESIDENTIAL ELECTORS
 for ALL Cast Vote Records before Election Day -- in Recorded Order
 PIMA County 2020 -- Final Ratio is 1.57



19. This graph and the graphs of this ratio in 16 additional contests all show a consistent pattern that would not exist in independent data without artificial manipulation. After an initial fluctuation due to the small number of votes counted at first, the cumulative Democrat/Republican ratio over time as additional votes were recorded in the CVR public record report closely followed a downward sloping line. For the Presidential race this decline was from over 300% down to 157% by Election Day.³

20. Very small deviations from a downward

³ The common opinion that Democrats vote earlier than Republicans would not explain the lack of independence between the data in the CVR graph.

sloping straight line indicate tight (strong) control, whereas wide deviations indicate weak or no control.

21. Since the effect of each additional vote on the cumulative ratio decreases as the number of votes increases, the deviation from a negative linear slope must be weighted in inverse proportion to the number of votes counted so far.

22. Also, to avoid the initial fluctuations due to the small number of votes at first, the following analysis begins after 50,000 votes, which is approximately 12% of the number of early votes recorded prior to November 3, 2020.

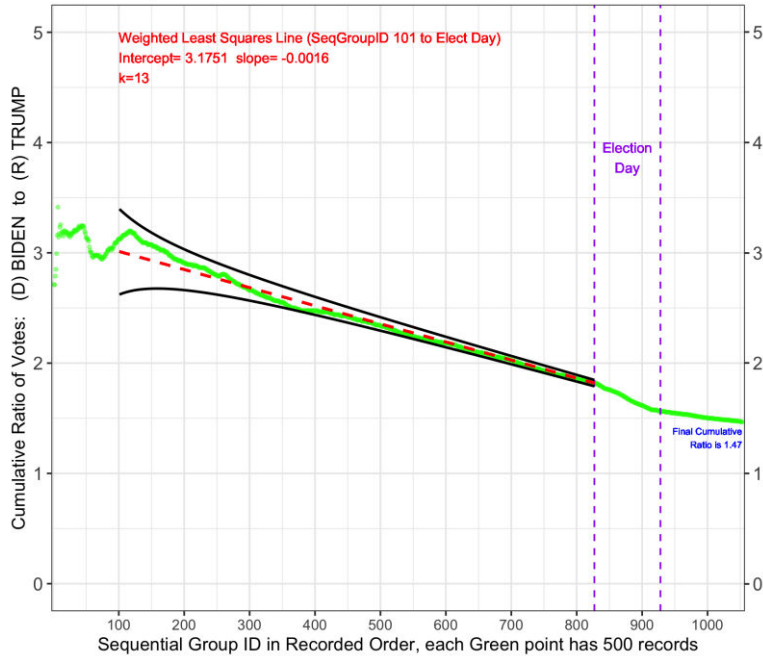
23. For the Presidential race, the least-squares linear regression trend line (the red dashed line in the following graph) has the equation

$$y = -0.0016x + 3.1751$$

where x is the sequential Group ID number.

120a

Cumulative Ratio of Votes: (D) BIDEN -to- (R) TRUMP
 Contest: PRESIDENTIAL ELECTORS
 for ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
 PIMA County 2020 -- Final Ratio is 1.47



24. Note how closely the actual CVR data (in green) follows the red trend line. To determine exactly how closely, we add the black boundary “curbs” (which must be weighted as described in ¶ 21) and find the narrowest curbs that contain all the green points. Also, as stated above, to avoid the initial fluctuations due to the small number of votes at first, the following analysis begins after 50,000 votes.

25. As in the graph in ¶ 18, ballots are grouped sequentially in batches of size 500 (Group 1 contains ballots 1-500, Group 2 contains ballots 501-1000, etc., in exactly the same order as recorded in the CVR records), so the last Group before Election Day is Group 826. (See ¶ 16 for how it was determined that

there were approximately 413,239 early votes counted prior to Election Day.)

26. To quantify the degree of control, the pair of narrowing black boundary lines in this graph shows a fixed percentage of deviation above and below a linear slope, weighted by the number of votes counted so far.

27. The boundary line equations are

$$y = (-0.0016x + 3.1751) \left(1 \pm \frac{k}{x}\right)$$

making $\frac{100k}{x}$ the percentage of deviation above and below a negative linear slope weighted by the number of votes counted so far. By testing integral values of k , it was determined that setting $k = 13$ is the minimum value such that the black boundaries include *all* the green data points, making the maximum percentage deviation at Election Day only $\frac{100 \cdot 13}{826} = 1.57\%$, an extremely close fit.

28. In statistical terms, the R^2 value for the red dashed line is 0.993, meaning that 99.3% of the total variation in the cumulative ratio is accounted for by the sequential Group number.

29. This means that after 50,000 votes out of a total of 413,239 early vote ballots have been counted, the cumulative Democrat/Republican ratio then follows a straight sloping line so closely that it must have been controlled.

30. Put another way, after about 12% of the early votes are recorded, the next block of ballots is 75% for the Democrat candidate, the next block after that is 74%, the next block 73%, and so on, systematically declining all the way to Election Day.

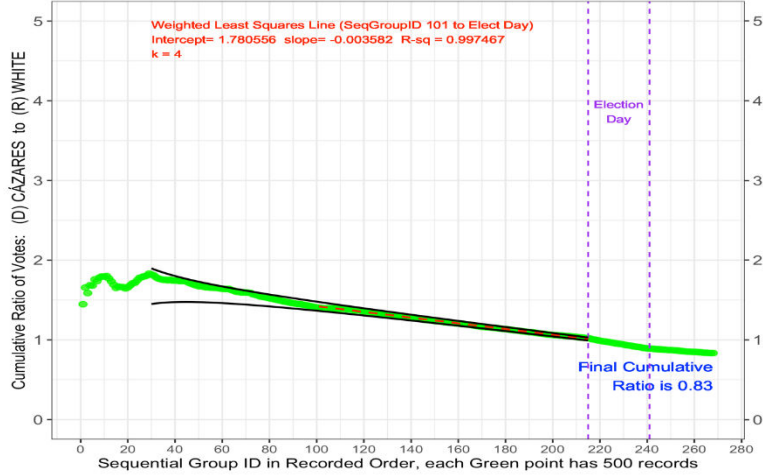
31. After approximately the first twelve percent

of votes are tabulated, the early votes are predictable and dependent in the relationship between one block of votes and the next. 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 without manipulation or control and thus demonstrates to a reasonable degree of scientific and mathematical certainty that the tabulation of these ballots was artificially controlled.

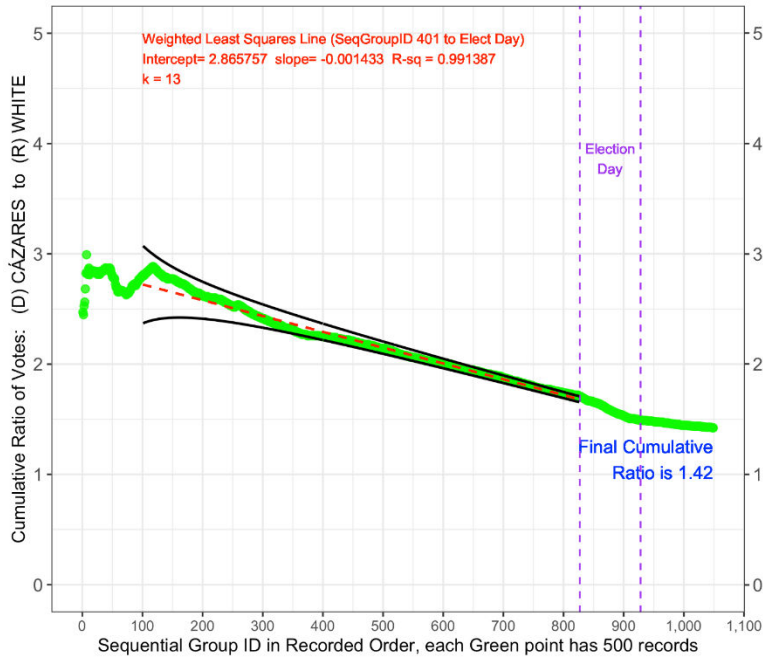
32. For confirmation, below are two additional graphs, one for Board of Supervisors District 4, and one for County Recorder, which are similarly predictable. The boundary curbs were also added, and the R^2 values for the red dashed lines are 0.997 and 0.991, respectively, confirming that over 99% of the total variation in the cumulative ratio is accounted for by the sequential Group number in both races.

123a

Cumulative Ratio of Votes: (D) DIAMOND -to- (R) CHRISTY
Contest: BOARD OF SUPERVISORS, DIST. 4
for ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 -- Final Ratio is 0.83



Cumulative Ratio of Votes: (D) CÁZARES -to- (R) WHITE
Contest: COUNTY RECORDER
for ALL Cast Vote Records (CVRs) in Sequential Groups of Size 500
PIMA County Arizona 2020 -- Final Ratio is 1.42



33. Note that neither the current Arizona statutory election audit procedures⁴ nor the various forms of risk-limiting audits used by other states would have detected this controlled manipulation, since they do not take into account the sequence that votes are recorded.

34. The standard method of producing such control as described above is to use a Proportional-Integral-Derivative (PID) controller in a closed-loop feedback system. As noted above, PID controllers are used everywhere, from cruise control in automobiles to Category III autoland for an aircraft making a landing when the runway is completely fogged in, to industrial automation of all kinds, such as robots, refineries and other chemical plants, manufacturing quality control, and self-driving cars.

35. By using all three factors (Proportional, Integral, and Derivative), a PID controller is the simplest (and therefore the most widely-used) design which controls both steady-state and transient responses, that is, it is able to reach and maintain a predetermined setpoint (outcome) despite unplanned disturbances. For example, in a Category III autoland situation when the airport is completely fogged in, the PID controller aims the aircraft for the start of the runway on a 3° glide slope, but if a sudden gust of wind pushes the nose down, the PID controller will activate the control surfaces to increase attitude and get back on the desired glide slope.

36. As a proof of concept I programmed a PID controller with a linearly-ramping__decreasing

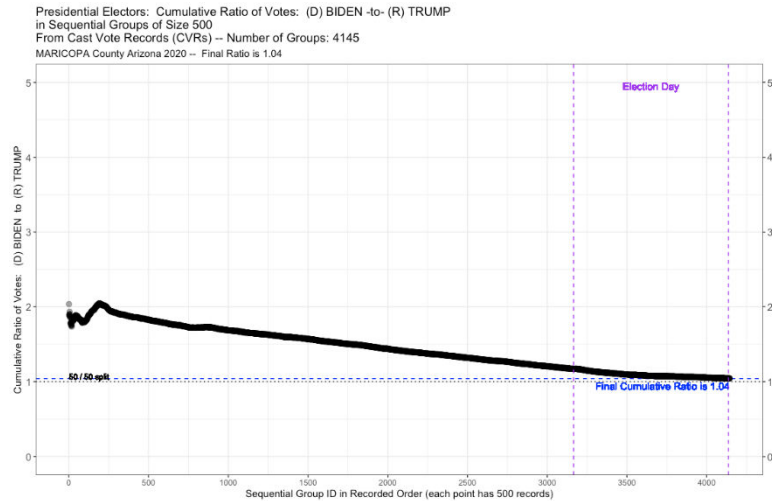
⁴ Arizona Revised Statutes Title 16. Elections and Electors § 16-602.

setpoint (the red dashed line) to produce the observed cumulative ratio and obtained good convergence after tuning the PID parameters to $K_p = 0.070$, $K_i = 0.300$, and $K_d = 0$. The system was not optimum (it was underdamped) but it was stable (with no unbounded oscillation) and closely tracked the continuing downward setpoint change along the red dashed line. Since the other 16 races had the same inexplicable downward slope, they would also match the same PID controller using their corresponding linearly-ramping decreasing setpoints.

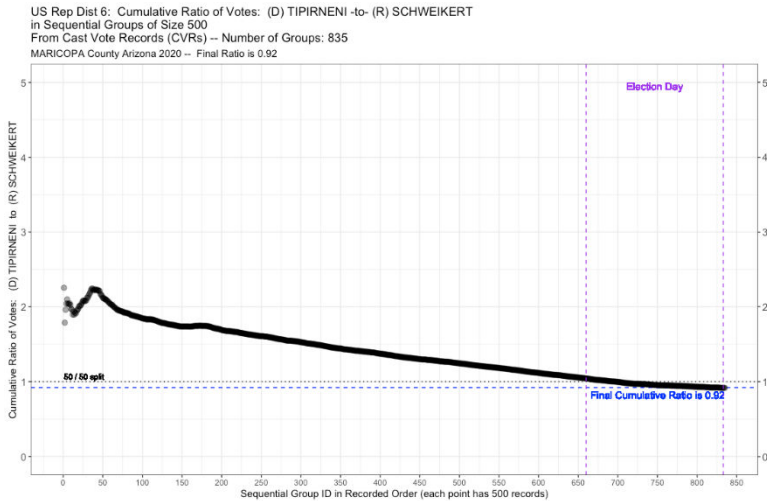
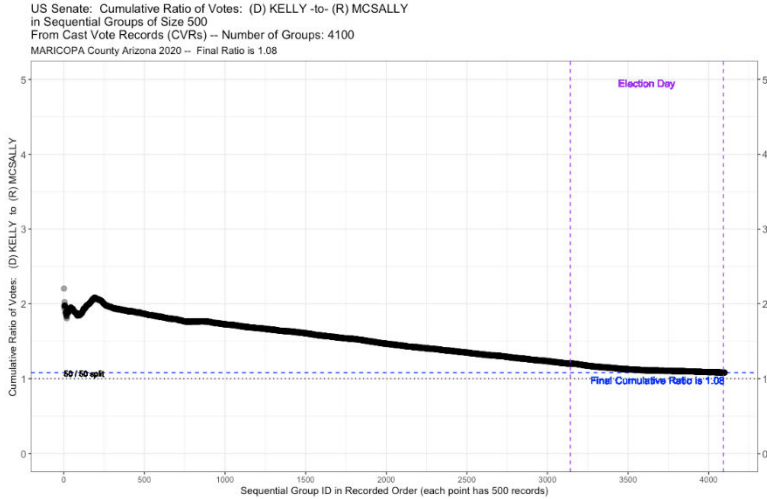
Early Vote Counting Was Manipulated In Maricopa County, Arizona

37. CVR data for all 10 federal races in Maricopa County, Arizona, was also received. However, since most of U.S. Representative District 1 lies outside Maricopa County, it was excluded from the following.

38. The same analysis as described above in ¶ 12-32 was performed on the remaining 9 federal races. Here are the graphs of the cumulative Democrat/Republican ratio for three of those races:



126a



39. Note that not only are the graphs almost identical to one another in shape, but they are also almost identical to the graphs from Pima County in ¶ 18 and ¶ 32, down to the twin peaks at the beginning and the “hiccup” when about 25% of the early votes have been counted.

40. For the Presidential race the ratio declined from about 1.9 down to 1.2 by Election Day.

**Consistency with Pima County
Whistleblower's Allegations**

41. My analysis above is based on the data that I reviewed, and not on any consideration of specific allegations of fraud. It was brought to my attention on May 4, 2022, subsequent to the analysis described above, that a Pima County whistleblower's email previously received by Plaintiff Finchem and others included allegations consistent with, and corroborative of, my conclusions. The whistleblower's full email is attached as Exhibit B. My independent analysis stands separate from this email, but the similarity between the allegations in the email and the result of my analysis is interesting.

Conclusions

42. The evidence detailed above overwhelmingly demonstrates to a reasonable degree of scientific and mathematical certainty that the sequence of the CVR data in both Maricopa County and Pima County shows artificial control.

43. Such control could be implemented by manual means or by a computer algorithm, such as a PID controller or some equivalent mathematical procedure. However, the alternating oscillations above and below the trend line, with decreasing deviations from the trendline, would require a prohibitive amount of calculation to accomplish by hand, not to mention the careful manual sorting of many thousands of batches of ballots to achieve the actual curves observed in the 26 races analyzed. This means that some type of computer algorithm is indicated, and a PID controller is the simplest control function that would exhibit following a trend line with alternating oscillations above and below

the trend line with decreasing deviations from the trendline.

44. Note that this same type of manipulation occurred both in Pima County, Arizona, which used ES&S voting machines (as did most other counties in Arizona), and also in Maricopa County, Arizona, which used Dominion voting machines (as did 23 other states), indicating that the same (or similar) software was responsible. Such manipulating software could be installed in a variety of ways, including vendor programming, operating system components, open-source or commercial off-the-shelf libraries, remote access, viruses or other malware, etc.

45. Unless and until future proposed electronic voting systems (including hardware, software, source code, firmware, etc.) are made completely open to the public and also subjected to scientific analysis by independent and objective experts to determine that they are secure from manipulation or intrusion, in my professional opinion as a computer expert, electronic voting systems should not even be considered for use in any future elections, as they cannot be relied upon to generate secure and transparent election results free from the very real possibility of unauthorized manipulation. My professional opinion as a computer expert is therefore that hand-marked hand-counted paper ballots should be used instead.

46. I have personal knowledge of the foregoing and am fully competent to testify to it at trial.

129a

I declare under penalty of perjury that the foregoing
is true and correct. Executed on June 8, 2022.

/s/ Walter C. Daugherty
Walter C. Daugherty

**UNITED STATES DISTRICT COURT
DISTRICT OF ARIZONA**

Kari Lake, *et al.*,
Plaintiffs,

v.

Katie Hobbs, Arizona
Secretary of State, *et al.*,
Defendants.

No. 2:22-cv-00677-JJT

DECLARATION OF BENJAMIN R. COTTON

I, Ben Cotton, being duly sworn, hereby depose and state as follows:

1. I am over the age of 18, and I understand and believe in the obligations of an oath. I make this affidavit of my own free will and based on first-hand information and my own personal observations.

2. I am the founder of CyFIR, LLC (CyFIR).

3. I have a master's degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

4. I have over twenty-six (26) years of experience performing computer forensics and other digital systems analysis.

5. I have over nineteen (19) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the

Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6. I have testified as an expert witness in state courts, federal courts and before the United States Congress.

7. I have testified before the Arizona State Senate in public hearings on 15 July 2021 and 24 September 2021 concerning the digital forensics findings connected to the Arizona State Senate Maricopa County audit of the 2020 general elections. I fully stand behind those forensic findings. I have included my presentation to the State Senate, file name Senate Final Presentation.pdf, as Exhibit A to this affidavit.

8. I regularly lead engagements involving digital forensics for law firms, corporations, and government agencies and am experienced with the digital acquisition of evidence under the Federal Rules of Evidence.

9. In the course of my duties I have forensically examined Dominion Democracy Suite voting systems in Maricopa County Arizona, Antrim County Michigan, Mesa County Colorado, and Coffee County Georgia, hereinafter referred to as the “Analyzed Elections Systems”.

10. In the course of my duties I have reviewed the administrative manuals and documentation for the Dominion Democracy Suite software and hardware components.

11. In the course of my duties I have reviewed the public information from the Election Assistance Commission and its certification process for election software.

12. I have reviewed and considered applicable

Arizona law¹ concerning the certification and operation of electronic voting systems².

13. I have reviewed and considered the Pro V&V report dated 3/2/2022 concerning the programmatic errors of the Dominion tabulator titled “ICP Modification to Reset Provisional Flag on each Ballot Scan”.

14. I have reviewed and considered Exhibits A through J in forming my opinion.

15. I have reviewed and considered the Maricopa Board of Supervisors’ Response to the Arizona Senate dated 5-17-21 and named “2021.05.17 Response Letter to Senate President Fann - FINAL_202105171430291332.pdf”.

16. I have reviewed and considered the published Department of Homeland Security, Cyber Security & Infrastructure Security Agency (CISA) Best Practices for Securing Election Systems dated 1 February 2021 and last revised on 25 August 2021. Publicly available, this document can be located at <https://www.cisa.gov/tips/st19-002>. This document provides recommendations for securing election systems in the following areas:

- a) Software and Patch Management – Note: The Analyzed Election Systems do not Comply with CISA Recommendations
- b) Log Management - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

¹ Arizona Revised Statutes Title 16. Elections and Electors

²

[https://azsos.gov/sites/default/files/2019 ELECTIONS PRO
CEDURES MANUAL APPROVED.pdf](https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf)

- c) Network Segmentation - Note: The Analyzed Election Systems Partially Comply with CISA Recommendations
- d) Block Suspicious Activity - Note: The Analyzed Election Systems do not Comply with CISA Recommendations
- e) Credential Management - Note: The Analyzed Election Systems do not Comply with CISA Recommendations
- f) Baseline Establishment for Host and Network Activity - Note: The Analyzed Election Systems do not Comply with CISA Recommendations
- g) Organization-Wide IT Guidance and Policies – Note: The Analyzed Election Systems Comply with CISA Recommendations
- h) Notice and Consent Banners for Computer Systems – Note: The Analyzed Election Systems Comply with CISA Recommendations

17. In addition, in forming my opinions, I reviewed and considered Exhibits B, C, D, E, F, G, H, I, and J, of which true and accurate copies are also attached hereto.

18. Based on my reviews of these documents, my cyber security experience, and my forensic analysis and review of the Dominion voting systems experience I find the following specific to the Cyber Security protections observed in the examinations of the Dominion Democracy Suite:

- a) Failure to Update Antivirus Protections - Based on my personal knowledge and experience, over one million (1,000,000) new malicious code samples are identified on a daily basis. It is imperative to the security of any computing system or enterprise that the antivirus definitions be updated as they become

available, typically on a weekly basis. There is a systemic issue with all of the Analyzed Elections Systems. There was an antivirus program installed on each of the systems. None of the system's antivirus definitions had EVER been updated following the installation of the Dominion Democracy Suite Software. In terms of the Maricopa County election system, the antivirus software had not been updated for over 19 months. In practical terms, this means that the virus protection was so out of date that the system would not have prevented over five hundred seventy million (570,000,000) pieces of malicious code from compromising the voting system.

b) Failure to Patch and Maintain Operating System (OS) Security – The

operating systems within the Analyzed Election Systems, including Windows, Linux and MacOS, contained vulnerabilities. These vulnerabilities could be exploited to gain unauthorized access to the targeted systems. Microsoft, the developer of the Windows software that was present on the Dominion PC-based Voting systems during my examination, releases operating system patches on a weekly basis to correct previously unknown operating system vulnerabilities and to prevent the possibility of unauthorized access to these systems. Based on my analysis of the Analyzed Election Systems in Maricopa County Arizona, Maricopa County Arizona, Fulton County Georgia, Antrim County Michigan, Mesa County Colorado, and Coffee County Georgia, there is no evidence of a procedure or process to patch or fix

the operating system vulnerabilities on the voting systems. None of these organizations had patched the operating systems

since the date that the Dominion Democracy Suite had been installed. In Maricopa County, the Windows operating systems had not been patched for over 19 months and contained fixes (patches) for three thousand five hundred twelve (3,512) known vulnerabilities directly applicable to the Maricopa County Dominion voting system. A list of these vulnerabilities is included as a file included with this report named, "Microsoft Patched Vulnerabilities between August 2019 and April 2021.xlsx (md5 hash value: D1E09A7C762E21653B1A28C3D9EE4E5E).

c) Failure to Properly Establish and Control Assess to Voting Systems - Based

on my review and consideration of the Analyzed Election Systems from different jurisdictions it is apparent that there is a systemic problem with access controls to the voting systems. In each case the usernames and passwords were established concurrently with the installation of the voting software by the Dominion employees. There are two major issues with the password management of these systems. First, in all examinations of the Analyzed Election Systems, the passwords were identical for all user accounts on that unique system. For each unique jurisdiction, all passwords within that election system were the same for all user accounts. Second, these passwords were never changed by the local officials following the installation of the software. These two deficiencies result in long-

term shared password exposure for multiple elections. Furthermore, there does not appear to be any accountability or assignment of the accounts to a specific individual for specific time periods. This makes individual accountability for actions performed by the account during an election impossible. CISA and industry best practices recommend that all username and password combinations be unique to each individual user. When that individual no longer requires access to the system, the username should be disabled to prevent unauthorized access to the system. When a new user arrives or is assigned, a new username and password are created for that user. Furthermore, CISA best practices dictate that each individual password should be changed every ninety (90) days. In the case of the Maricopa County devices, the passwords had not been changed for over nineteen (19) months, and no user accounts had ever been created following the installation of the Dominion software.

- d) No Process Monitoring, Network Monitoring or Baseline Monitoring – Based on my review of the electronic voting systems from different jurisdictions, none of the jurisdictions had the capability to actively monitor programs that were running on the computers, monitor network activity, or had a process to alert election officials if a deviation from an approved baseline occurred.
- e) Log Management – Retaining and adequately securing logs from both network devices and local hosts is a critical component of cyber security. Not only does a robust log management

program support the detection and monitoring of real-time security postures, but in the event of an audit or a cyber security event, these logs support triage and remediation of the historical cybersecurity events. None of the election systems that I have examined have an independent log management program. An effective log management program should include the following capabilities:

- i) Centralized Log Management: It is common for threat actors to delete, modify and/or otherwise manipulate logs and other artifacts as an integrated element of an unauthorized attack. An effective log management program would establish a centralized log repository that is not located on the device that generates the logged event. This method allows for potentially unlimited log retention time periods, assurance of log preservation, ensures the integrity of the logs, and establishes a data repository to aid in the detection of malicious behavior. None of the election systems that I have analyzed forwarded logs to a centralized log management server.
- ii) Security Information and Event Management – A security information and event management tool is commonly referred to as a SIEM. I have personal experience with and have observed threat actors attempting to delete local logs to remove on-site evidence of their activities, including log deletion, log modification and changing logging settings. By sending logged events to a SIEM tool, an organization can reduce the likelihood of malicious log spoilation and maximize the ability to detect malicious

activity. None of the election systems that I have analyzed utilized a SIEM.

- iii) Effective log correlation from both network and host security devices is critical to protecting election networks and computing devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the entire organization. Modern log analysis and correlation systems provide the analysis, detection of an anomaly, and alerting within 15 seconds from event to eyes on glass by an analyst. None of the election systems that I have analyzed were capable of log correlation.
- iv) Review both centralized and local log management policies to maximize efficiency and retain historical data. CISA recommends that organizations retain critical logs for a minimum of one year, if possible. Federal law³ requires that all election system-related logs be retained for at least 22 months. In the case of the Maricopa County election system analysis, the Election Management Server (EMS) contained two hundred thirty-seven (237) distinct Windows-specific log files and three hundred fifty-two (352) archived Dominion Democracy Suite logs. The Dominion Democracy Suite logs appear to have been preserved in accordance with the Federal retention statute, but of the two hundred thirty-seven (237) distinct Windows-specific log files only three were produced in

³ US Code 52 Section 20701 - Retention and Preservation of Records and Papers by Officers of Elections; Deposit with Custodian; Penalty for Violation.

response to the subpoena. Among the missing were the critical Windows security.evtx log. It is critical that all system and application-specific logs be independently retained in accordance with the federal, state, and local statutes. Centralized logging also addresses potential logging and log retention issues discovered during the analysis of the Maricopa County election system. In all examined systems, the Windows operating system event logs were set to the default Windows log size of 20 megabytes. When the maximum file size is reached, for every new logged event that is created, the oldest log entry is deleted. This ensures that the actual log file never exceeds 20 megabytes. The issue arises over time if the logs are not forwarded to a centralized log server, then logged events are lost over time. In the event of the Maricopa County analysis, the oldest logged event in the security.evtx log file was dated 5 February 2021. Thus, the log did not encompass the 2020 General Election time frame.

- v) PowerShell and Advanced Logging Should be Enabled
- (1) PowerShell is a cross-platform command-line shell and scripting language that has quickly become a central exploitation capability by malicious actors. I have personally observed threat actors, including advanced persistent threat (APT) actors, using PowerShell to exploit systems and hide their malicious activities.
- (2) Given the extensive usage of PowerShell to exploit systems by malicious actors, it is imperative that the PowerShell instances have

module, script block, and transcription logging enabled.

- f) Network Segmentation – In all the election systems that I have examined I identified an attempt to segment the systems that record the votes from the systems that administratively support the voting process, (e.g. poll worker laptops, voter registration data base, etc.). Segmentation was attempted by using an “air gap” to isolate the Dominion Democracy Suite systems. This partially complies with the CISA Best Practices for Securing Election Systems. The issue is the overreliance on the air gap to provide segmentation and security to a network. It is a false assumption that, because there is no connection to the internet by an internal router the network is fully segmented and secure. History has proven that air-gapped systems are easily bypassed by connecting cell phones, wireless “hockey pucks”, other wireless networks to an endpoint internal to the air gapped systems. It is important to note that all the computers used within the Dominion Democracy Suite are commercial off-the-shelf (COTS) hardware from Dell computers. A search of a subset of these systems indicates that these systems do contain wireless 802.11 modems that can connect to unauthorized networks if the user has administrative access. As all of the accounts, including the administrative accounts, had the exact same password, any user of the system could have thwarted the air gap security in a matter of seconds. As previously mentioned, in the systems that I have examined there would

not have been any mechanism to detect or prevent such a violation of the system security.

- g) Block Suspicious Activity – In every election system that I have analyzed there has been no mechanism for blocking malicious activity or programs other than the outdated antivirus program. Given the lack of operating system patching, lack of antivirus definition updating, and the lack of password controls, the Analyzed Election Systems, as examined, simply do not have the ability to detect or block suspicious activity.

19. Updating election systems, subsequent system configuration, and subsequent system validation of election systems is an inherent government function of the local voting jurisdiction. Government officials must provide competent and continuous oversight of vendors supporting the updating and certification of those systems to comply with the appropriate jurisdictional requirements and regulations. In order to perform these oversight functions, the government must have full control and the same levels of administrative access as the vendors in order to access detailed information concerning the full scope/impacts of the vendor activities. This level of access and control is required to be able to independently validate that those contractors do not violate the law. I have discovered in the course of my work on the Analyzed Election Systems that the vendors of election software did not allow the counties to control or possess the authentication mechanisms that would permit independent validation of the system's configuration prior to certification. Simply put, there currently is no mechanism for county clerks to independently

validate the installation of firmware, system configurations, determine the status and configuration of wireless devices, or other program installations without relying solely on the vendor-provided data or data provided by a company closely associated with the software vendor as the basis for certification. This was the case in Maricopa County. In order to validate the configuration of the Dominion ICP ballot tabulators, including the ability to determine if a wireless modem was enabled or disabled, a technician password was required. In response to the Senate request for the technician password, the Board of Supervisors replied in paragraph 3 of the Maricopa County Board of Supervisor's Response to Arizona Senate questions dated 5-17-21 and named "2021.05.17 Response Letter to Senate President Fann - FINAL_202105171430291332.pdf" that the county did not possess that password, nor could the county compel production of that password from the Dominion employees. Therefore, it would have been impossible for the County Board of Supervisors to independently validate the ICP configuration for local certification of the voting system or to ensure that the configuration of the systems was changed after the system was certified.

20. Based on my experience if the Cyber Security failures and lapses exhibited by the election systems networks and computers that I have examined were present in an enterprise that was subject to PCI or HIPAA industry certifications, that network would not be certifiable.

SIGNED UNDER THE PAINS AND PENALTIES
OF PERJURY THIS 8th DAY OF JUNE 2022.

143a

/s/ signed

Benjamin R. Cotton

Exhibit A - Senate Final Presentation Exhibit B -
CyTech Taiwan Germany

Exhibit C - 2021.05.17 Response Letter to Senate
President Fann - FINAL_202105171430291332

Exhibit D - 033122 EAC Dominion Anomoly

Exhibit E - Antrim Lawsuit Exhibit 8 Benjamin
Cotton Affidavit Exhibit F - 081920 Halderman
Declaration

Exhibit G - 080221 Halderman Decl. Exhibit H -
Special Master Final Report Exhibit I - EMS
Windows Log Files

Exhibit J - Microsoft Patched Vulnerabilities
between August 2019 and April 2021

144a

2:22-CV-00677-JJT, JULY 21, 2022

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Kari Lake, et al.,
Plaintiffs,

v.

**Katie Hobbs, named
as Kathleen Hobbs,
as Secretary of
State, et al.,**

Defendants.

2:22-cv-00677-JJT

Phoenix, Arizona
July 21, 2022
9:06 a.m.

BEFORE:

THE HONORABLE JOHN J. TUCHI, JUDGE

REPORTER'S TRANSCRIPT OF PROCEEDINGS
MOTION HEARING

Official Court Reporter

Elaine Cropper, RDR, CRR, CCP

Sandra Day O'Connor U.S. Courthouse

401 West Washington Street

Suite 312, SPC 35

Phoenix, Arizona 85003-2150

(602) 322-7245

Proceedings Reported by Stenographic Court Reporter

Transcript Prepared by Computer-Aided Transcription

United States District Court

[* * *]

[Pages 19:16 – 29:12, Cotton]

Q. In terms of the components that you were not provided authentication in order to get in and analyze, did you ask to be provided with that information? Did you indicate that it was important to your review?

A. We did and we did that on multiple occasions. What ultimately came back both, in public and private statements by the County, was that the county did not actually control those authentications, those eye button tokens, that would permit to us get access to the technician or the administrative functions of the system. The only people who had access and control of those were the Dominion employees who were on site at the County.

Furthermore, the County indicated that they could not compel the Dominion employees to produce those eye buttons or tokens. So, therefore, we were not allowed or we did not get access to confirm the configurations of the wireless modems, the LANs and those such devices as they were configured on the tabulators.

Q. But you made it clear that you wanted access?

A. Yes.

Q. Now, the vendor is Dominion Voting Systems in Maricopa?

A. Correct.

Q. And you say they had control of providing the access?

A. Yes. And the concern on that, obviously, is that inherently the validation of the certification of

the systems and the validation of those tabulators should be an intergovernmental function by Maricopa County personnel. And if they don't have access to do that that, then that means that they are relying on the goodness and kindness and accurate reporting of the Dominion employees.

Q. In terms of what you were able to get and look at in the -- under the hood, if you will, of the electronic voting system used in Maricopa, what did you find when you looked in terms of any security vulnerability?

MR. GAONA: Objection, Your Honor. I just want to note for the record, given the pending motion, that we do have an objection to Mr. Cotton providing expert testimony on this issue under Rule 702, a Daubert decision, as well as maintaining our relevance and 403 objections. I just want to note a standing objection for the record on that issue with respect to his opinions.

THE COURT: You may.

MR. GAONA: Thank you.

THE COURT: All right. You may proceed.

MR. PARKER: No need for me to respond to that at this point, Your Honor.

THE COURT: No. You are going to respond in writing and I know you're in the middle of your examination now, so we will establish a timeline for the response before we leave here today.

Go ahead, sir.

MR. PARKER: Thank you.

THE WITNESS: Quite frankly, I was shocked at the lack of cybersecurity elements within the voting system and I'll give you a couple of examples of that.

So if I was to summarize this, I would say that the average home computer is better protected than the EMS and the client systems that were in the Maricopa County environment.

BY MR. PARKER:

Q. And why do you say that?

A. Well, let me back that up. So when you -- when you look at a computer, you have a layered line of defenses because cybersecurity is an ongoing continual effort and there's no one security mechanism that is going to be completely bulletproof. In the case of Maricopa County, they primarily relied on an air gap system and that air-gap system, given the configuration of those other components of the enterprise, could be bypassed in about 30 seconds.

We'll probably go into that a little bit further. So once you get past that air gap, then you have to rely on on-prem type of devices like antivirus. Now, the EAC does require the antivirus on the system. But in the case of Maricopa County, the definitions of that antivirus had not been updated since August 6 of 2019. I examined the systems in April and May of 2021.

So the business importance on that is that from my experience as a cybersecurity expert, there are over one million pieces of malware that are either generated, modified or newly equipped with signatures changed every day. And so when you look at this, there were, you know, just off the top of my head, roughly 700 million pieces of malware out there that the Maricopa County systems would not detect by their antivirus.

Furthermore --

Q. What about patches, updates?

A. System patches are an essential element of cybersecurity.

As we know, Microsoft is one of the largest producers of system software in the world. In its systems, with the exception of the tabulators, for all of the computer devices that were turned over to me they were running, they went by version of Windows software. They had the Dominion software as an application on that device but underlying this was Windows.

Every week Microsoft will release a vulnerability patch update. That's because even Microsoft doesn't know all of the vulnerabilities that exist in their own operating system, and people find these vulnerabilities that can allow them to get remote access and exploit the systems. And Microsoft will patch those and they do that on a weekly basis. Depending on where you are, that's typically Wednesday or Thursday.

They also provide an off-line service for these patches so that you don't have to connect to the Internet to download them and put them on your systems.

Q. When was the last time those patches were updated or added at all?

A. The same date that they installed the software, which was August 6, 2019.

Q. No patches since then and you looked at it in 2021?

A. Correct. There were well over a thousand known vulnerabilities that could have been exploited by a kiddie scriptor with a program called Metasploit or some other exploit

tool. It wouldn't have taken any skill.

Q. What about passwords, were those protected?

A. So they did have a password. And the reason I use "a password" was they used the same password for every single account on the domain on the system.

Q. And you saw this yourself?

A. I did.

Q. With respect to the antivirus, the patches, and the passwords, you saw all of that yourself?

A. Yes, I did. And I used -- I examined the forensics images. I used forensically court-approved tools to perform that analysis, and those images are available for other experts to look at if they should request.

Q. So if the passwords are the same for all people getting access, is that a proper protection mechanism?

A. No. And furthermore, it wasn't just it was the same password, it's that the password was established at the time of the installation of the software and it had not been changed since it was installed.

So that same password had been used for all accounts from August 2019 until the time that I examined the system.

Q. So if you had that password, could you get into the EMS system?

A. You could, either locally or, if you had remote access, you could log in remotely to the system.

Q. What about log management activity in the system? Did you assess that?

A. I did and, quite frankly, they had left the default sizes for all of the logs.

So the way that works is that I'm going to use the Windows security log, for example. On the server version of Microsoft, that is set at 20 megabytes and when a new log entry comes in, the oldest log entry is deleted and thrown away.

When I examined -- from that forensics image I took of the EMS server, the latest -- or the furthest back that that log went was 5 February 2021.

Q. Post election?

A. Post election the County had turned over some logs but missing was the Windows security log. There were approximately 79 different entries or different log types on the Windows operating system side and they turned over three Windows-specific logs to the Senate. But they did not turn over the application log or the security log.

The issue with that is that that is the log that actually records the remote accesses to the system, the IP addresses from which that remote access occurs and the user that performs that remote access.

Q. And so were logs overwritten post election or did you have the election time period logs?

A. Well, the logs were -- the term that I would use were rolling the logs, so the logs were rolled in the case of the Windows security log.

On three separate occasions, the first occasion being on the -- I believe it was the fifth of February. There were about 462 instances of a script being ran that ran to check for a blank password. Now, there are only about 15 accounts on the system. So they

ran that 462 times.

The next occasion was on the third of March and they ran that same script over 34,000 times. And then on the 12th of April, which was right before they were turning the devices over to the Senate, they ran that approximately three hundred and some times. The net result of that activity was that the Windows security log only went back to the fifth of February.

Q. And were you ever provided with some sort of a secure data set from when the election occurred that might have been saved or backed up or mirror imaged?

A. I was not. That was actually an issue between the Senate and the County as to the full compliance on the subpoena.

Q. Any other maladies or issues you found in terms of the security in the system when you looked at the Maricopa County electronic voting machine system?

A. Yes. So there is a -- I have personally viewed a line in the Arizona code that remote access to those systems shall not be enabled. There shall be no program on those systems that would allow remote access.

On all of the systems that I examined, the Microsoft Remote Desktop application was still on the systems and that was used to remotely log in to the server on multiple times.

Q. So you saw actual evidence of remote intervention?

A. I saw actual evidence of remote log-ins into the EMS server.

Q. And do you know whether those were permissible or security breach or . . .

A. The attributable log-ins -- because I did see some anonymous log-ins that I could not trace back to an event. The ones that I saw came from the local EMS subnet, if you will, the IP address that -- for the voting system.

Q. Since we're talking about intrusion into the system through remote access, air gap is a term that you used a little bit earlier. Is that a process to prevent or limit remote access?

A. It is an attempt to limit a remote access. I would say that it's a good step but it's not bulletproof. It's easily bypassed.

Everyone in here probably owns a cell phone and whether it's IOS or whether it's Android based that cell phone would have a function called personal hotspot where you can use your cell phone as a wifi connector to the outside.

The issue with that becomes, is that each of the Dell computers that were within that system did have wifi cards and that those wifi cards had been registered as a network on the computing devices.

So what that means is that at the time they installed the software, those wifi cards were not disabled in BIOS. Otherwise, they would not have been recognized by the operating system.

But the other interesting fact is, if you set up a wifi without a password, then it is -- the default configuration for Windows to automatically connect to an unprotected wifi system.

Q. Is that a description of a hotspot? If somebody gained access, they could utilize the hotspot to gain

access?

A. Sure, yeah. That would give access to the Internet. You know, there are multiple examples of breaches through air-gap systems. If you remember the Snowden breach of the NSA, that was an air-gap system.

Q. That the NSA had set up?

A. That the NSA had set up.

Q. And Snowden breached it?

A. Correct.

Q. You would assume it was a hardened system?

A. Yes.

Q. It was breached, nonetheless?

A. Yes.

Q. Other examples?

A. Stux -- S-T-U-X -- net is an example and that was a piece of malware that was designed to be delivered via USB. It would iterate a network, promulgate itself until it reached a centrifuge, and then control the speed of the centrifuge in order to destroy the centrifuge.

Q. Have you heard the phrase or statement made by cybersecurity experts that given enough time and access, any computer system can be hacked?

A. Yes.

Q. Do you agree with it?

A. I certainly do, especially if you have physical access to those systems.

[* * *]

[Pages 114:03-118:03, Parikh]

DIRECT EXAMINATION

BY MR. PARKER:

Q. Good afternoon, sir. State your name, please, and spell your last name for the record.

A. My name is Clay Parikh, P-A-R-I-K-H.

Q. And Mr. Parikh, what is your current employment?

A. I am with Northrop Grumman. I'm the Lead Information Systems Security Officer for the Ground Missile Defense System.

Q. And how long have you been at Northrop?

A. Just over two years.

Q. Where did you work before that?

A. I was with Leidos and also Lockheed Martin at the time of transition.

Q. So they are the same company?

A. What? Lockheed Martin sold off the division to Leidos in a merger.

Q. How long were you with Lockheed Martin/Leidos?

A. Ten years.

Q. And what work did you do for them?

A. I was the Deputy Cybermanager for the Army Corps of Engineers.

Q. Have you done any work for accredited testing labs in the U.S. EAC protocols?

A. Yes, sir. From 2008 to 2017 I worked in Bode System Test Labs.

Q. And which -- were you a contractor?

A. Yes, sir, I was a contractor.

Q. And what was your title?

A. I was the security subject matter expert.

Q. So were you the one that did testing on electronic voting machines?

A. Yes, sir. And to be more specific, I did the security testing.

Q. And would you say you've done a hundred or more security tests?

A. Yes, sir.

Q. And these are on electronic voting machines like ES&S and Dominion Voting Systems?

A. Yes, sir.

Q. Was this a part of the certification process for EAC?

A. Yes, it was and also for Secretaries of State.

Q. Do you have any certifications?

A. Yes, sir. I have the CISSP which is a Certified Information Systems Security Professional. Then I also have the Certified Ethical Hacker and I'm also a Certified Hacking Forensics Investigator.

Q. Is a central piece of your job to hack into electronic voting machines?

A. Yes.

Q. And this was from 2008 to 2017; correct?

A. That is correct.

Q. Did you ever have occasion to be testing or hacking into Dominion Voting Systems?

A. Yes, sir.

Q. And a number of times?

A. Repeatedly.

Q. Were you able to hack into the systems?

A. Yes, sir, I was.

Q. How long would it take you to do that?

A. On average, five to ten minutes.

Q. And what would you ES&D systems, were you able to – or did you have occasion to test and try to hack into ES&D systems?

A. Yes, sir.

Q. And were you able to do that?

A. Yes, sir, I was.

Q. Repeatedly?

A. Repeatedly.

Q. Over all of those years?

A. Yes, sir and I tested other voting systems by other vendors as well.

Q. How long would it take you to hack into the ES&S system?

A. I think my best time was two and a half minutes. On average, though, it was usually five to ten minutes. It really didn't make a difference on the vendor.

Q. And then would you record that information that you were able to hack in?

A. Yes, sir.

Q. And, again, this was part of the EAC certification process?

A. Yes, it was.

Q. So you reported this up the chain for the purpose of the process?

A. All my reports and findings were given to the voting system test labs.

Q. Now, have you had occasion to look at the Dominion Voting Systems that they are intending to use in 2022?

A. I have reviewed that analysis and reports of the systems that have been done up to date to include Maricopa County's report and I find that they are the same configuration of those versions that I tested previously.

Q. That you were able to hack into in five to ten minutes?

A. Yes, sir.

Q. And what about ES&S and their configuration, have you reviewed those?

A. Yes, I have.

Q. And are those configurations the same as what you reviewed as intended to be used in Arizona?

A. Yes.

Q. Which of the accredited testing labs did you work for between 2008 and 2017 as a contractor?

A. I worked for Wiley laboratories which then transitioned into NTS and then I worked for Pro V&V.

MR. PARKER: I have nothing further, Your Honor.

THE COURT: All right. Thank you, Mr. Parker.

Mr. Gaona, do you have questions for this witness?

MR. GAONA: A couple, Your Honor. Yes.

THE COURT: Okay.

UnclearBallot: Automated Ballot Image Manipulation

Matthew Bernhard, Kartikeya Kandula, Jeremy Wink, and J. Alex Halderman

Department of Electrical Engineering and Computer Science, University of Michigan
{matber, kartkand, jr Jeremy, jhalderm}@umich.edu

Abstract. As paper ballots and post-election audits gain increased adoption in the United States, election technology vendors are offering products that allow jurisdictions to review ballot images—digital scans produced by optical-scan voting machines—in their post-election audit procedures. Jurisdictions including the state of Maryland rely on such image audits as an alternative to inspecting the physical paper ballots. We show that image audits can be reliably defeated by an attacker who can run malicious code on the voting machines or election management system. Using computer vision techniques, we develop an algorithm that automatically and seamlessly manipulates ballot images, moving voters’ marks so that they appear to be votes for the attacker’s preferred candidate. Our implementation is compatible with many widely used ballot styles, and we show that it is effective using a large corpus of ballot images from a real election. We also show that the attack can be delivered in the form of a malicious Windows scanner driver, which we test with a scanner that has been certified for use in vote tabulation by the U.S. Election Assistance Commission. These results demonstrate that post-election audits must inspect physical ballots, not merely ballot images, if they are to strongly defend against computer-based attacks on widely used voting systems.

Keywords: optical scan, paper ballots, image manipulation, drivers, image processing

1 Introduction

Elections that cannot provide sufficient evidence of their results may fail to adequately gain public confidence in their outcomes. Numerous solutions have been posited to this problem [9], but none has been as elegant, efficient, and immediately practical as post-election audits [21, 25, 39]. These audits—in particular, ones that seek to limit the risk of confirming an outcome that resulted from undue manipulation—are one of the most important layers of defense for election security [32].

Risk-limiting audits (RLAs) rely on sampling robust, independent evidence trails created by voter-verified paper ballots. However, other types of post-election

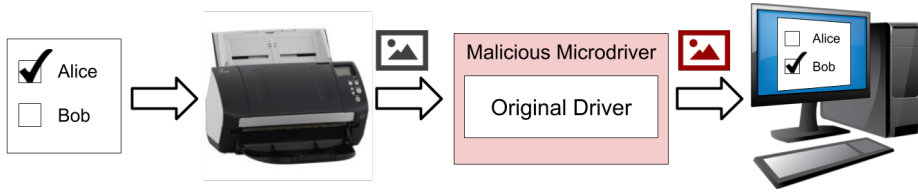


Fig. 1. Attack overview—A voter’s paper ballot is scanned by a ballot tabulator, producing a digital image. Malware in the tabulator—in our proof-of-concept, a microdriver that wraps the scanner device driver—alters the ballot image before it is counted or stored. A digital audit shows only the manipulated image.

audits are gaining popularity in the marketplace. In particular, Clear Ballot, an election technology vendor in the United States, pioneered audit software designed to perform audits of *images* of ballots which have been scanned and tabulated, which we shall refer to as “image audits”. Other vendors have adopted support for this kind of audit, and one U.S. state, Maryland, relies on image audits to provide assurances of its election results [33].

While image audits can help detect human error and aid in adjudicating mismarked ballots, we show that they cannot provide the same level of security assurance as audits of physical ballots. Since ballot images are disconnected from the actual source of truth—physical paper ballots—they do not necessarily provide reliable evidence of the outcome of an election under adversarial conditions.

In this paper, we present UnclearBallot, an attack that defeats image audits by automatically manipulating ballot images as they are scanned. Our attack leverages the same computer vision approaches used by ballot scanners to detect voter selections, but adds the ability to move marks from one target area to another. Our method is robust to inconsistent or invalid marks, and can be adapted to many ballot styles.

We validate our attack against a corpus of over 180,000 ballot images from the 2018 election in Clackamas County, Oregon, and find that UnclearBallot can move marks on 34% of the ballots while leaving no visible anomalies. We also test our attack’s flexibility using six widely used styles of paper ballots, and its robustness to invalid votes using an established taxonomy of voter marks. As a proof-of-concept, we implement the attack in the form of a malicious Windows scanner driver, which we test using a commercial-off-the-shelf scanner certified for use in elections by the U.S. Election Assistance Commission.

UnclearBallot illustrates that post-election audits in traditional voting systems must involve rigorous examination of *physical ballots*, rather than ballot images, if they are to provide a strong security guarantee. Without an examination of the physical evidence, it will be difficult if not impossible to assure that computer-based tampering has not occurred.

The remainder of this paper is organized as follows: Section 2 provides background on image audits, ballot scanners, and image processing techniques we use to implement our attack. Section 3 describes the attack scenarios against

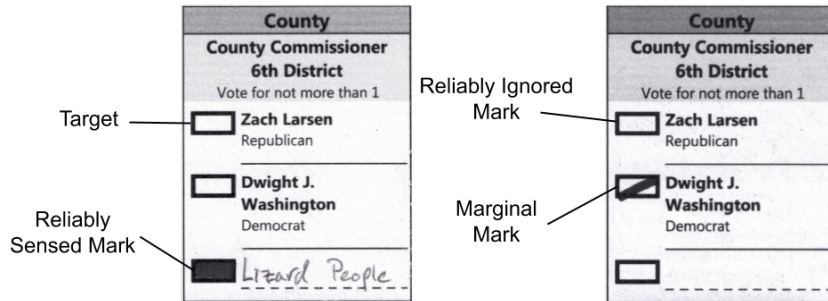


Fig. 2. Terms for parts of a marked ballot, following Jones [23].

optical scanners and image audits. Section 4 explains the methodology of our attack. In Section 5 we present data indicating that our attack can be robust to various ballot styles and voter marks. Section 6 contextualizes our attacks and discusses mitigations. We conclude in Section 7.

2 Background

Our attack takes advantage of two aspects of optical scanner image audits: the scanning and image processing techniques used by scanners, and the reliance on scanned images by image audits. Here we provide a brief discussion of both.

2.1 Ballot Images

Jones [23] put forth an analysis of the way that ballot scanners work, particularly the mark-sense variety that is most common today. All optical scanners currently sold to jurisdictions, as well as the vast majority of scanners used in practice in the U.S., rely on mark-sense technology [44]. Scanners first create a high-resolution image of a ballot as it is fed past a scan head. Software then analyzes the image to identify dark areas where marks have been made by the voter.¹ Once marks have been detected, systems may use template matching to translate marks into votes for specific candidates, typically relying on a barcode or other identifier on the ballot that specifies a ballot style to match to the scanned image.

Detecting and interpreting voter marks can be a difficult process, as voters exhibit a wide range of marking and non-marking behavior, including not filling in targets all the way, resting their pens inside targets, or marking outside the target. The terms Jones developed to refer to the ballot and marks are illustrated in Figure 2. Marks that adequately fill the target and are unambiguously interpreted as votes by the scanner are called *reliably sensed* marks, and targets that are unambiguously not filled and therefore not counted are *reliably ignored* marks.

¹ The details of how marks are identified vary by hardware and scanning algorithm. See [13] for an example.



Fig. 3. Taxonomy of voter marks adapted from Bajcsy [2], including the five leftmost marks that may be considered marginal marks.

Marks of other types are deemed *marginal*, as a scanner may read or ignore them. Moreover, whether a mark should be counted as a vote is frequently governed by local election statute, so some marginal marks may be unambiguously counted or ignored under the law, even if not by the scanner.

Bajcsy et al. [2] further develops a systematization of marginal marks and develops some improvements on mark-detection algorithms to better account for them. An illustration of Bajcsy et al.’s taxonomy is shown in Figure 3. Ji et al. [22] discuss different types of voter marks as applied to write-in votes, as well as developing an automated process for detecting and tabulating write-in selections.

2.2 Image Audits

Risk-limiting post-election audits rely on physical examination of a statistical sample of voter-marked ballots [24, 26, 39, 40]. However, this can create logistical challenges for election officials, which has prompted some to propose relaxations to traditional audit requirements. To reduce workload, canvass audits and recounts in many states rely on retabulation of ballots through optical scanners (see the 2016 Wisconsin recount, for example [31]).

Some election vendors take retabulation audits a step further: rather than physically rescan the ballots, the voting system makes available images of all the ballots for independent evaluation after the election [15, 16, 42].² While the exact properties of these kinds of image audits vary by vendor, they typically rely on automatically retabulating all or some images of cast ballots, as well as electronic adjudication for ballots with marginal marks. These “audits” never examine the physical paper trail of ballots, which our attack exploits.

Several jurisdictions have relied on these image audits, including Cambridge, Ontario, which used Dominion’s AuditMark [17], and the U.S. state of Maryland, which uses Clear Ballot’s ClearAudit [28]. Maryland has also codified image audits into its election code, requiring that an image audit be performed after every election [27].

² While the review is made available to the public, the actual images themselves are seldom published in full out of concern for voter anonymity.

3 Attack Scenarios

Elections in which voters make their selections on a physical ballot are frequently held as the gold standard for conducting a secure election [32]. However, the property that contributes most to their security, software independence [34], only exists if records computed by software are checked against records that cannot be altered by software without detection. Image audits enable election officials to view images of ballots and compare them with the election systems' representation of the particular ballot they are viewing (called a cast vote record or CVR). While these two trails of evidence may be independent from each other (for example, Clear Ballot's ClearAudit [15] technology can be used to audit a tabulation performed by a different election system altogether), they are not software independent. A clever attacker can exploit the reliance on software by both evidence trails to defeat detection.

To surreptitiously change the outcome of the election in the presence of an image audit, the attacker must alter both the tabulation result as well as the ballot images themselves. Researchers have documented numerous vulnerabilities that would allow an attacker to infect voting equipment and change tabulation results (see [10, 20, 30] among others), so we focus on the feasibility of manipulating ballot images once an attacker has successfully infected a machine where they are stored or processed.

The most straightforward attack scenario occurs when the ballot images are created by the same equipment that produces the CVR. In this case, the attacker can simply infect the scanner or tabulator with malware that corrupts both the CVR and the images at the same time. The attack could change the image before the tabulator processes it to generate the CVR, or directly alter both sets of records.

In some jurisdictions, the ballot images that are audited are collected in a separate process from tabulation—that is, by scanning the ballots again, as in Maryland's use of ClearAudit from 2016 [28]. In this case, the adversary has to separately attack both processes, and has to coordinate the cheating to avoid mismatches between the initial tally and the altered ballot images.

Depending on the timing of the audit, manipulation of ballot images need not be done on the fly. For example, if the ballot images are created during tabulation but the image audit does not occur until well after the election, an attacker could modify the ballot images while they are in storage.

For ease of explication, the discussion that follows assumes that ballot images are created at the time of tabulation, in a single scan. The attack we develop targets a tabulation machine and manipulates each ballot online as it is scanned.

4 Methodology

To automatically modify ballot images, an attacker can take a few approaches. One approach would be to completely replace the ballot images with ballots filled in by the attacker. However, this risks being detected if many ballots have

the same handwriting, and requires sneaking these relatively large data files into the election system without being detected. For these reasons, we investigate an alternative approach: automatically and selectively doctoring the ballot scans to change the vote selections they depict.

For the attack to work successfully, we need to move voter marks to other targets without creating visible artifacts or inconsistencies. We must be able to dynamically detect target areas and marks, alter marks in a way that is consistent with the voter’s other marks, and do so in a way that is undetectable to the human eye. However, there is a key insight that works in the adversary’s favor: an attacker seeking to alter election results does not have to be able to change *all* ballots undetectably, only sufficiently many to swing the result. This means that the attacker’s manipulation strategy is not required to be able to change *every* mark—it merely has to reliably detect *which* marks it can safely alter and change enough of them to decide the election result.

4.1 Reading the ballot

To interpret ballot information, we rely on the same techniques that ballot scanners use to convert paper ballots into digital representations. Attackers have access to the ballot templates, as jurisdictions publish sample ballots well ahead of scheduled elections. Using template matching, an attacker does not have to perform any kind of sophisticated character recognition, they simply have to find target areas and then detect which of the targets are filled.

Our procedure to read a ballot is illustrated in Figure 4. First, we perform template matching to extract each individual race within a ballot. Next, we use OpenCV’s [11] implementation of the Hough transform to detect straight lines that separate candidates and break the race into individual panes for each candidate. Notably, the first candidate in each race may have the race title and extra information in it (see Figure 4c), which is cropped out based on white space.

Target areas are typically printed on the ballot as either ovals or rectangles. To detect them, we construct a bounding box around the target by scanning horizontally from the left of the race and then vertically from the bottom up, and compute pixel density values. The bounds are set to the coordinates where the density values first increase and last decrease. Once we have detected all the target areas, we compute the average pixel density of the area within the bounding box to determine whether or not a target area is marked. We then use our template to convert marks into votes for candidates.

4.2 Changing marks

Once we have identified which candidate was marked by the voter, we can move the mark to one of the other target locations we identified. If the vote is for a candidate the attacker would like to receive fewer votes—or if it is not a vote for a candidate they would like to win—the attacker can simply swap the pixels within the bounding boxes of the voter’s marked candidate and an unmarked candidate.

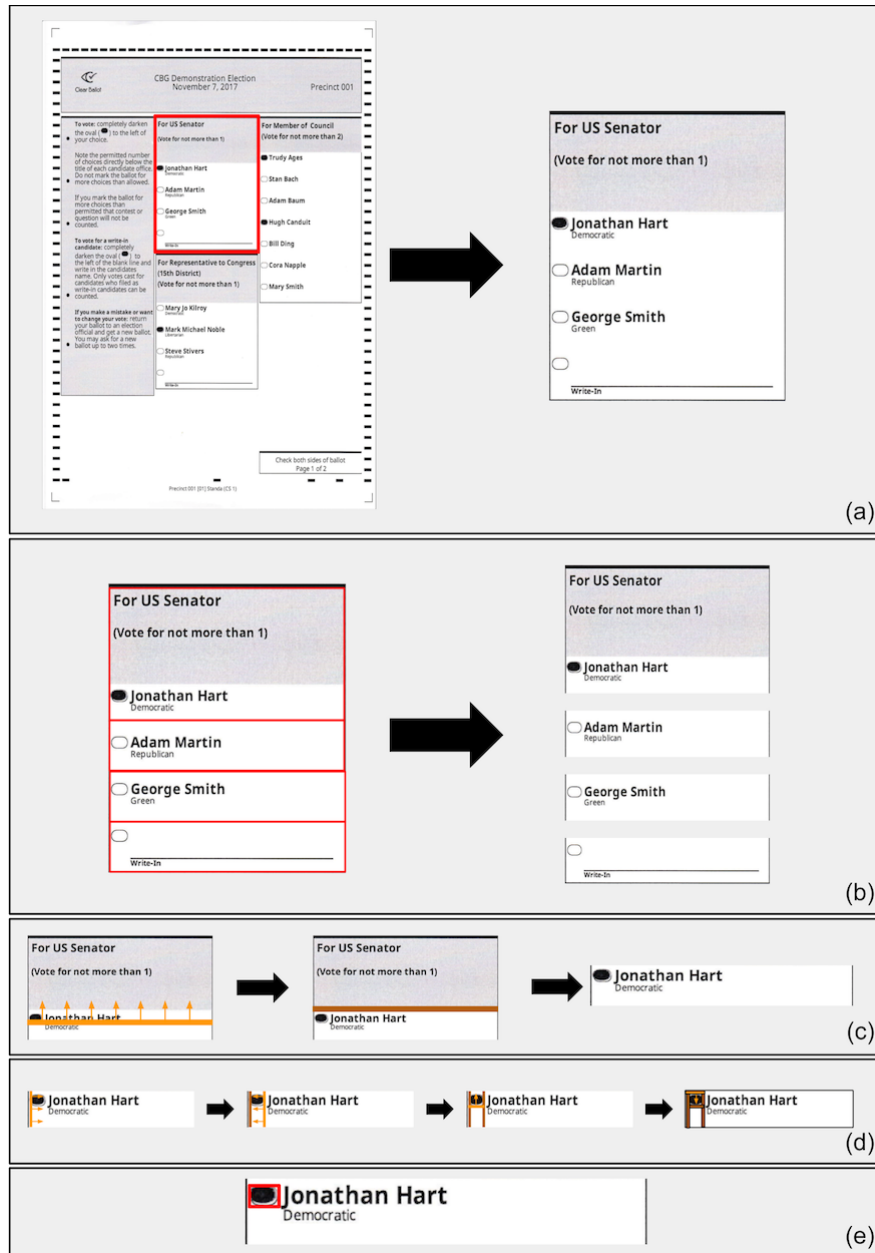


Fig. 4. Ballot manipulation algorithm—First, (a) we apply template matching to extract the race we intend to alter. Then, (b) we use Hough line transforms to separate each candidate. If the first candidate has a race title box, (c) we remove it by computing the pixel intensity differences across a straight line swept vertically from the bottom. For each candidate, (d) we identify the target and mark (if present) by doing four linear sweeps and taking pixel intensity. Finally, (e) we identify and move the mark. At each step we apply tests to detect and skip ballots where the algorithm might leave artifacts.





Original		Manipulated	
County		County	
Supervisor, District 1		Supervisor, District 1	
Vote for One		Vote for One	
Alfred Hitchcock		Alfred Hitchcock	<input type="radio"/>
Vincent Price	<input type="radio"/>	Vincent Price	
Write In	<input type="radio"/>	Write In	<input type="radio"/>
State		State	
Governor		Governor	
Vote for One		Vote for One	
Amelia Earhart	<input type="radio"/>	Amelia Earhart	
Howard Hughes		Howard Hughes	<input type="radio"/>
Charles Lindbergh	<input type="radio"/>	Charles Lindbergh	<input type="radio"/>
Write In	<input type="radio"/>	Write In	<input type="radio"/>

Fig. 5. Automatically moving voter marks—UnclearBallot seamlessly moves marks to the attacker’s preferred candidate while preserving the voter’s marking style. It is effective for a wide variety of marks and ballot designs. In the examples above, original ballot scans are shown on the left and manipulated images on the right.

By moving marks on each ballot separately, we ensure that the voter’s particular style of filling in an oval is preserved and consistent across the ballot. Figure 5 shows some marks swapped by our algorithm, and how the voters original mark is completely preserved in the process.

4.3 UnclearBallot

To illustrate the attack, we created UnclearBallot, a proof-of-concept implementation packaged as a malicious Windows scanner driver, which consists of 398 lines of C++ and Python. We tested it with a Fujitsu fi-7180 scanner (shown in Figure 6), which is federally certified for use in U.S. elections as part of Clear Ballot’s ClearVote system [43]. These scanners are typically used to handle small volumes of absentee ballots, and must be attached to a Windows workstation that runs the tabulation software.

The UnclearBallot driver wraps the stock scanner driver and alters images from the scanner before they reach the election management application. We chose this approach for simplicity, as the Windows driver stack is relatively easy



Fig. 6. The **Fujitsu fi-7180 scanner** we used to test our attack has been certified by the U.S. Election Assistance Commission for use in voting systems. Our proof-of-concept implementation is a malicious scanner driver that alters ballots on the fly.

to work with, but the attack could also be implemented at other layers of the computing stack. For instance, it could be even harder to detect if implemented as a malicious change to the scanner’s embedded firmware. Alternatively, it could be engineered as a modification to the tabulation software itself.

Once a ballot is scanned, the resulting bitmap is sent to our image processing software, which manipulates the ballot in the way described in Section 4.1. Prior to the election, the attacker specifies the ballot template, which race they would like to affect, and by how much. While ballots are being scanned, the software keeps a running tally of the actual ballot results, and changes ballot images on the fly to achieve the desired election outcome. To avoid detection, attackers can specify just enough manipulated images so that the race outcome is changed.

5 Evaluation

We evaluated the performance and effectiveness of UnclearBallot using two sets of experiments. In the first set of experiments, we marked different ballot styles by hand using types of marks taxonomized by Bajcsy et al. [2]. In the second set of experiments, we processed 181,541 ballots from the 2018 election in Clackamas County, Oregon.

5.1 Testing Across Ballot Styles

In order for our application to succeed at its goal (surreptitiously changing enough scanned ballots to achieve a chosen election outcome), it must be able to detect marks that constitute valid votes as well as distinguish marks which would be noticeable if moved. The marks in the latter case represent a larger set than just marginal marks, as they may indeed be completely valid votes, but considered invalid by our mark-moving algorithm. For example, if we were to swap the targets on a ballot where the user put a check through their target, we may leave a significant percentage of the check around the original target when swapping. The same applies for marked ballots where the filled in area extends into the candidate’s name, which could lead our algorithm to swap over parts of the candidate’s name when manipulating the image.

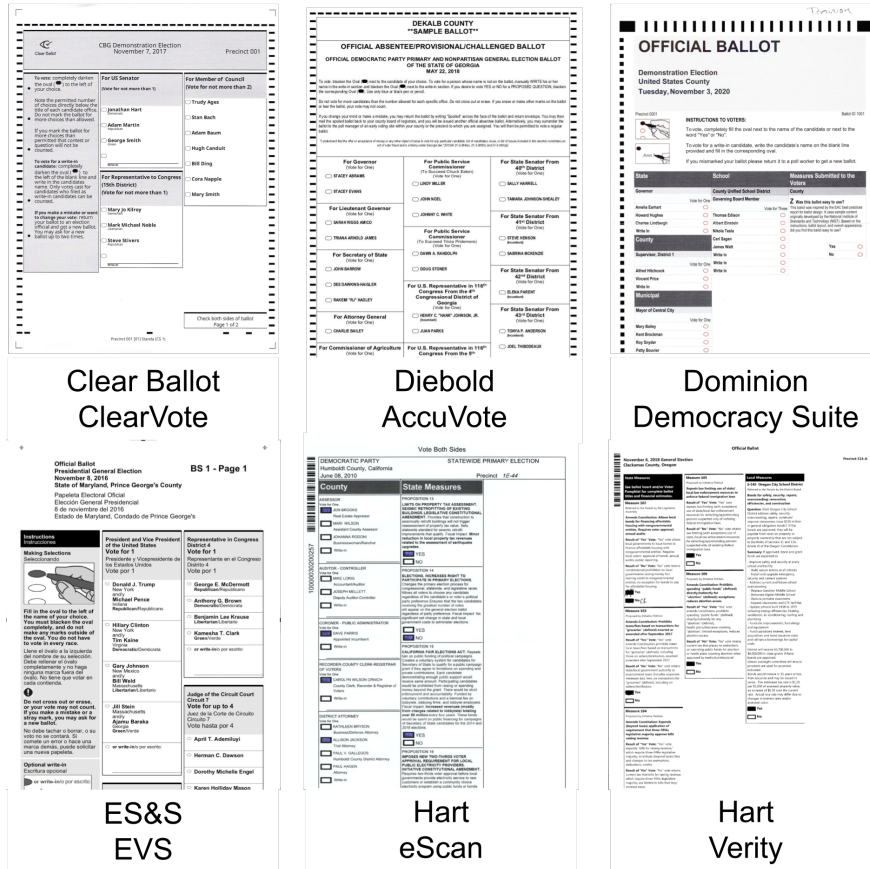


Fig. 7. Ballots Styles— We tested ballot designs from five U.S. voting system vendors: Clear Ballot, Diebold, Dominion, ES&S, and Hart (two styles, eScan and Verity).

To detect anomalies for invalid ballots, we leverage the same intensity checking algorithm that first found the marked areas. The program checks if the width or height is abnormally large, which would indicate an overfilled target, as well as if there are too few or too many areas of high intensity, which would indicate no target or too many targets are filled out. If the program detects an invalid ballot, it will not be modified by the program.

To show our attack is replicable on a variety of different ballot styles, we modified our program to work on six different sample ballot styles, shown in Figure 7. The ballots we tested come from the four largest election vendors in the U.S. (ES&S, Hart InterCivic, Dominion, and Clear Ballot), as well as two older styles of ballots from Hart and Diebold.

Our first experiment was designed to characterize the technique’s effectiveness across a range of ballot styles and with both regular and marginal marks. We

Ballot Style	Invalid Marks			Valid Marks			Time/Success
	Skipped	Success	Failure	Skipped	Success	Failure	
Clear Ballot	55	5	0	26	34	0	25 ms
Diebold	60	0	0	6	54	0	11 ms
Dominion	38	22	0	7	53	0	30 ms
ES&S	52	8	0	29	31	0	54 ms
Hart (eScan)	60	0	0	38	22	0	46 ms
Hart (Verity)	60	0	0	27	33	0	21 ms

Table 1. Performance of UnclearBallot — We tested how accurately our software could manipulate voter marks for a variety of ballot styles using equal numbers of invalid and valid marks. The table shows how often the system skipped a mark, successfully altered one, or erroneously created artifacts we deemed to be visible upon manual inspection. We also report the mean processing time for successfully manipulated races, excluding template matching.

prepared 720 marked contests, split evenly among the six ballot styles shown in Figure 7. For each style, we marked 60 contests with what Bajcsy [2] calls “Filled” marks, i.e. reliably detected marks that should be moved by our attack. We marked another 60 ballots in each ballot style with marginal marks, ten each for the five kinds of marginal marks shown in Figure 2 and ten empty marks.

Because the runtime of the template matching step of our algorithm is highly dependent on customization for the particular races on a ballot, we opted to skip it for this experiment. Rather than marking full ballots, we marked cropped races from each ballot style and then ran them through our program. We then manually checked to ensure that the races the program moved were not detectable by inspection. Results for these experiments are shown in Table 1.

Despite rejecting some valid ballots, our program is still able to confidently swap a majority of valid votes. In a real attack, only a small percentage of votes would need to actually be modified, a task easily accomplished by our program. Our program also correctly catches all votes that we have deemed invalid for swapping. This would make it unlikely to be detected in an image audit.

Dominion ballots saw a much higher rate of invalid mark moving, and Diebold and Dominion ballots saw a much higher rate of valid mark moving. This is likely due to the placement of targets: on the Dominion ballots, the mark is right justified, separating it significantly from candidate label information, as can be seen in Figure 7. Similarly, the Diebold ballot provides more space around the target and less candidate information that can be intercepted by marks, which would cause Unclear Ballot to skip moving the mark.

In an online attack scenario (such as if a human is waiting to see the output from the scanner), the attacker needs to be able to modify ballot scans quickly enough not to be noticed. Factors which might affect how quickly our program can process and manipulate ballots include ballot style, layout, and type of mark. During the accuracy experiment just described, we collected timing data for

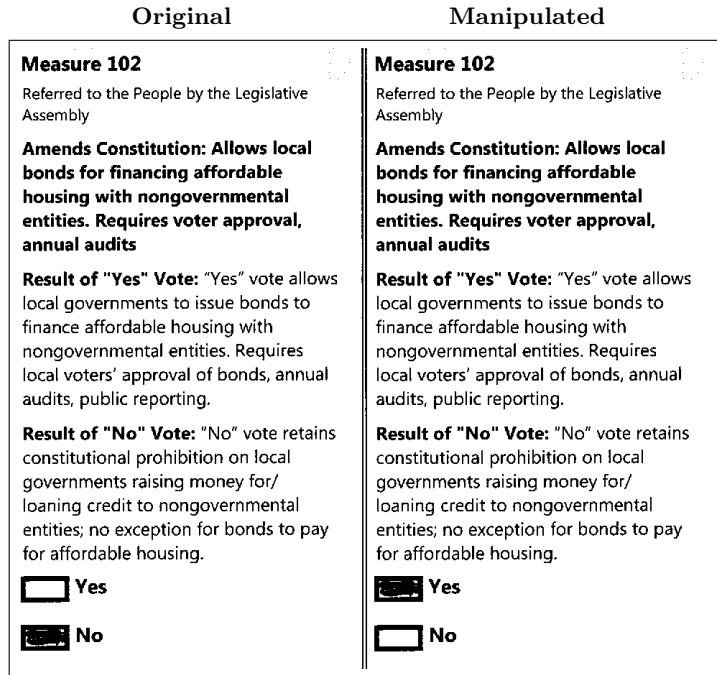


Fig. 8. Attacking Real Ballots—Using 181,541 images of voted ballots from Clackamas County, Oregon, we attempted to change voters' selections for the ballot measure shown above. UnclearBallot determined that it could safely alter 34% of the ballots. For reference, Measure 102 passed by a margin of 5%, well within range of manipulation [14]. We inspected 1,000 of them to verify that the manipulation left no obvious artifacts.

successfully manipulated ballot, and report the results in Table 1. The results show that after the target race has been extracted, the algorithm completes extremely quickly for all tested ballot styles. We present additional timing data at the end of the following section.

5.2 Testing with Real Voted Ballots

To assess the effectiveness of UnclearBallot in a real election, we used a corpus of scans of 181,541 real ballots from the November 6, 2018, General Election in Clackamas County, Oregon, which were made available by Election Integrity Oregon [18]. Like all of Oregon, Clackamas County uses vote-by-mail as its primary voting method, and votes are centrally counted using optical scanners. All images were Hart Verity-style ballots, as shown in Figure 7.

We selected a ballot measure that appeared on all the ballots (Figure 8) and attempted to change each voter's selection. UnclearBallot rejected 20,117 (11%) of the ballots because it could not locate the target contest. We examined a subset of the rejected ballots and found that they contained glitches introduced

during scanning (such as vertical lines running the length of the ballot), which interfered with the Hough transform.

To simulate a real attacker, we configured UnclearBallot with conservative parameters, so that it would only modify marks when there was high confidence that the alteration would not be noticeable. As a result, it would only manipulate marks that were nearly perfectly filled in. In most cases, marks that were skipped extended well beyond the target, but the program also skipped undervotes, overvotes, or mislabeled scans. Under these parameters, the program altered the target contest in 62,400 (34%) of the ballot images.

Two authors independently inspected a random sample of 1,000 altered ballots to check whether any contained artifacts that would be noticeable to an attentive observer. Such artifacts might include marks which were unnaturally cut off, visible discontinuities in pixel darkness (i.e. dark lines around moved marks), and so on. If these artifacts were seen during an audit, officials might recheck all of the physical ballots and reverse the effects of the attack. None of the altered ballots we inspected contained noticeable evidence of manipulation.

We also collected timing data while processing Clackamas County ballots. Running on a system with a 4-core Intel E3-1230 CPU running at 3.40 GHz with 64 GB of RAM, UnclearBallot took an average of 279 ms to process each ballot. For reference, Hart’s fastest central scanner’s maximum scan rate is one ballot per 352 ms [37], well above the time needed to carry out our attack.

These results show that UnclearBallot can successfully and efficiently manipulate ballot images to change real voters’ marks. Moreover, the alterations likely would be undetectable to human auditors who examined only the ballot images.

6 Discussion and Mitigations

UnclearBallot demonstrates the need for a software-independent evidence trail against which election results can be checked. It shows that audits based on software which is independent from the rest of the election system is still not software independent. To date, the only robust and secure election technology that is widely used is optical-scan paper ballots with risk-limiting audits based on a robust, well-maintained, *physical* audit trail. However, image audits are not useless, and here we discuss uses for them as well as potential mitigations for our attack.

Uses for image audits. So long as image audits are not the sole mechanism for verifying election results, they do provide substantial benefits to election officials. Using an image audit vastly simplifies some functions of election administration, like ballot adjudication in cases where marks cannot be interpreted by scanners or are otherwise ambiguous. Image audits can be used to efficiently identify and document election discrepancies, as has occurred in Maryland where nearly 2,000 ballots were discovered missing from the audit trail in 2016 [28]. Image audits also identified a flaw in the ES&S DS850 high speed scanner, where it was causing some ballots to stick together and feed two at a time [29].

Another way to utilize image audits is a transitive audit. Methods like SOBA [8] seek to construct an audit trail using all available means of election evidence, rooting the audit in some verification of physical record. By using physical records to verify other records, like CVRs or ballot images, confidence in election outcomes can be transitively passed on to non-physical audit trails. The drawback with this kind of audit is that it usually requires the same level of work as an RLA, plus whatever work is needed to validate the other forms of evidence. However, since ballot image audits already require a low amount of effort, they may augment RLAs and provide better transparency into the auditing process.

Image audits are an augmentation and a convenience for election administration, however, and should not be viewed as a security tool. Only physical examination of paper ballots, as in a risk-limiting audit, can provide a necessary level of mitigation to manipulated election results.

End-to-end (E2E) systems. Voting systems with rigorous integrity properties and tamper resistance such as Scantegrity [12] and Prêt à Voter [35] provide a defense to UnclearBallot. In Scantegrity, when individuals mark their ballots, a confirmation code is revealed that is tied to the selected candidate. This enables a voter to verify that their ballot collected-as-cast and counted-as-collected, as they can look up their ballot on a public bulletin board. Since each mark reveals a unique code, moving the mark would match the code with the wrong candidate, so voters would be unable to verify their ballots. If enough voters complain, this might result in our attack being detected.

Prêt à Voter randomizes the candidate order on each ballot, which creates a slightly higher barrier for our attack, as an additional template matching step would be needed to ascertain candidate order. More importantly, the candidate list is physically separated from the voter’s marks upon casting the ballot, so malware which could not keep track of the correct candidate order could not successfully move marks to a predetermined candidate. Since the candidate order is deciphered via a key-sharing scheme, malicious software would have to infect a significant portion of the election system and act in a highly coordinated way to reconstruct candidate ordering. Moreover, as with Scantegrity, votes are published to a public bulletin board, so any voter could discover if their vote had not been correctly recorded.

Other E2E systems which make use of optical scanning and a bulletin board, like STAR-Vote [6], Scratch and Vote [1], and VeriScan [7], are similarly protected from attacks like UnclearBallot.

Other mitigations. Outside of E2E, there may be other heuristic mitigations that can be easily implemented even in deployed voting systems to make our attack somewhat more difficult. As mentioned above, randomizing candidate order on each ballot increases the computation required to perform our attack. Voters drawing outside the bubbles can also defeat our attack, though this might also result in their votes not counting and may be circumvented by replacing the whole race on the ballot image with a substituted one. Collecting ballot images

from a different source than the tabulator makes our attack more difficult, as votes now have to be changed in two places. Other standard computer security technologies, like secure file systems, could be used to force the attacker to alter ballot images in a way that also circumvents protections like encryption and permissions.

Detection. Technologies that detect image manipulation may also provide some mitigation. Techniques like those discussed in [3–5, 38], among others, could be adapted to try to automatically detect moved marks on ballots. However, as noted by Farid [19], image manipulation detection is a kind of arms race: given a fixed detection algorithm, adversaries can very likely find a way to defeat it. In our context, an attacker with sufficient access to the voting system to implant a manipulation algorithm would likely also be able to steal the detector code. The attacker could improve the manipulation algorithm or simply use the detector as part of their mark-moving calculus: if moving a mark will trip the detector, an attacker can simply opt not to move the mark.

While a fixed and automatic procedure for detecting manipulation can provide little assurance, it remains possible that an adaptive approach to detection could be a useful part of a post-election forensics investigation. However, staying one step ahead of sophisticated adversaries would require an ongoing research program to advance the state of the art in detection methods.

A less costly and more dependable way to detect ballot manipulation detection would be to use a software independent audit trail to confirm election outcomes. This can be accomplished with risk-limiting audits, and the software independence enabled by RLAs provides other robust security properties to elections, including defending against other potential attacks on tabulation equipment and servers.

Future work. We have only focused on simple-majority elections here, because those are the kinds of elections used by jurisdictions that do image audits. Audits of more complex election methods, like instant-runoff voting or D’Hondt, have been examined to some extent [36, 41], but future work is needed into audits of these kinds of elections altogether. Because the marks made in these elections are different than the kind we’ve discussed here, manipulating these ballot images may not be able to employ the same image processing techniques we have used. Additionally it may be difficult for malware to know how many marks it needs to move, since margins in complex elections are difficult to compute. We leave exploration of image manipulation of these elections to future work.

7 Conclusion

In this paper, we demonstrated an attack that defeats ballot image audits of the type performed in some jurisdictions. We presented an implementation using a real scanner, and evaluated our implementation against a set of real ballots and a set of systematically marked ballots from a variety of ballot styles. Our

attack shows that image audits cannot be relied upon to verify that elections are free from computer-based interference. Indeed, the only currently known way to verify an election outcome is with direct examination of physical ballots.

Acknowledgements

The authors thank Vaibhav Bafna and Jonathan Yan for assisting in the initial version of this project. They also thank Josh Franklin, Joe Hall, Maurice Turner, Kevin Skoglund, Jared Marcotte, and Tony Adams for their invaluable feedback. We also thank our anonymous reviewers and our shepherd, Roland Wen. This material is based upon work supported by the National Science Foundation under grant CNS-1518888.

References

1. Adida, B., Rivest, R.L.: Scratch and Vote: Self-contained paper-based cryptographic voting. In: ACM Workshop on Privacy in the Electronic Society. pp. 29–40 (2006)
2. Bajcsy, A., Li-Baboud, Y.S., Brady, M.: Systematic measurement of marginal mark types on voting ballots. Tech. rep., National Institute for Standards and Technology (2015)
3. Bayar, B., Stamm, M.C.: A deep learning approach to universal image manipulation detection using a new convolutional layer. In: Proceedings of the 4th ACM Workshop on Information Hiding and Multimedia Security. pp. 5–10. ACM (2016)
4. Bayram, S., Avcibas, I., Sankur, B., Memon, N.: Image manipulation detection with binary similarity measures. In: 2005 13th European Signal Processing Conference. pp. 1–4. IEEE (2005)
5. Bayram, S., Avcibas, I., Sankur, B., Memon, N.D.: Image manipulation detection. *Journal of Electronic Imaging* **15**(4), 041102 (2006)
6. Bell, S., Benaloh, J., Byrne, M.D., DeBeauvoir, D., Eakin, B., Fisher, G., Kortum, P., McBurnett, N., Montoya, J., Parker, M., Pereira, O., Stark, P.B., Wallach, D.S., Winn, M.: STAR-vote: A secure, transparent, auditable, and reliable voting system. *USENIX Journal of Election Technology and Systems* **1**(1) (Aug 2013)
7. Benaloh, J.: Administrative and public verifiability: Can we have both? In: USENIX/ACCURATE Electronic Voting Technology Workshop. EVT '08 (Aug 2008)
8. Benaloh, J., Jones, D., Lazarus, E., Lindeman, M., Stark, P.B.: SOBA: Secrecy-preserving observable ballot-level audit. In: proc. Proc. USENIXAccurate Electronic Voting Technology Workshop (2011)
9. Bernhard, M., Benaloh, J., Halderman, J.A., Rivest, R.L., Ryan, P.Y., Stark, P.B., Teague, V., Vora, P.L., Wallach, D.S.: Public evidence from secret ballots. In: International Joint Conference on Electronic Voting. pp. 84–109. Springer (2017)
10. Bowen, D.: Top-to-Bottom Review of voting machines certified for use in California. Tech. rep., California Secretary of State (2007), <https://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/>
11. Bradski, G.: The OpenCV Library. *Dr. Dobb's Journal of Software Tools* (2000)
12. Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E., Sherman, A.T., Vora, P.L.: Scantegrity II municipal election at Takoma Park: The first E2E binding governmental election with ballot privacy. In: 18th USENIX Security Symposium (Aug 2010)

13. Chung, K.K.t., Dong, V.J., Shi, X.: Electronic voting method for optically scanned ballot (Jul 18 2006), US Patent 7,077,313
14. November 6, 2018 general election. <https://dochub.clackamas.us/documents/drupal/f4e7f0fb-250a-4992-918d-26c5f726de3c>
15. Clear Ballot: ClearAudit, <https://clearballot.com/products/clear-audit>
16. Dominion Voting: Auditmark. <https://www.dominionvoting.com/pdf/DD%20Digital%20Ballot%20AuditMark.pdf>
17. Dominion Voting: Cambridge Case Study. <https://www.dominionvoting.com/field/cambridge>
18. Election Integrity Oregon, <https://www.electionintegrityoregon.org>
19. Farid, H.: Digital forensics in a post-truth age. *Forensic science international* **289**, 268–269 (2018)
20. Feldman, A.J., Halderman, J.A., Felten, E.W.: Security analysis of the Diebold AccuVote-TS voting machine. In: USENIX/ACCURATE Electronic Voting Technology Workshop. EVT '07 (Aug 2007)
21. Hall, J., Miratrix, L., Stark, P., Briones, M., Ginnold, E., Oakley, F., Peaden, M., Pellerin, G., Stanionis, T., Webber, T.: Implementing risk-limiting post-election audits in California. In: 2009 Workshop on Electronic Voting Technology/Workshop on Trustworthy Elections. pp. 19–19. USENIX Association (2009)
22. Ji, T., Kim, E., Srikantan, R., Tsai, A., Cordero, A., Wagner, D.A.: An analysis of write-in marks on optical scan ballots. In: EVT/WOTE (2011)
23. Jones, D.W.: On optical mark-sense scanning. In: *Towards Trustworthy Elections*, pp. 175–190. Springer (2010)
24. Lindeman, M., Halvorson, M., Smith, P., Garland, L., Addona, V., McCrea, D.: Principles and best practices for post-election audits (Sep 2008), <http://electionaudits.org/files/bestpracticesfinal.0.pdf>
25. Lindeman, M., Stark, P.: A gentle introduction to risk-limiting audits. *IEEE Security and Privacy* **10**, 42–49 (2012)
26. Lindeman, M., Stark, P., Yates, V.: BRAVO: Ballot-polling risk-limiting audits to verify outcomes. In: 2011 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE '12). USENIX (2012)
27. Maryland House of Delegates: House Bill 1278: An act concerning election law – postelection tabulation audit. <http://mgaleg.maryland.gov/2018RS/bills/hb/hb1278E.pdf>
28. Maryland State Board of Elections: 2016 post-election audit report. http://dlslibrary.state.md.us/publications/JCR/2016/2016_22-23.pdf (12 2016)
29. Maryland State Board of Elections: December 15, 2016 meeting minutes. https://elections.maryland.gov/pdf/minutes/2016_12.pdf (Dec 2016)
30. McDaniel, P., Blaze, M., Vigna, G.: EVEREST: Evaluation and validation of election-related equipment, standards and testing. Tech. rep., Ohio Secretary of State (2007), <http://siis.cse.psu.edu/everest.html>
31. Mebane, W., Bernhard, M.: Voting technologies, recount methods and votes in Wisconsin and Michigan in 2016. 3rd Workshop on Advances in Secure Electronic Voting 2018 (2018)
32. National Academies of Sciences, Engineering, and Medicine: *Securing the Vote: Protecting American Democracy*. The National Academies Press, Washington, DC (2018), <https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy>
33. National Conference of State Legislatures: Post-election audits (January 2019), <http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx>

34. Rivest, R.: On the notion of ‘software independence’ in voting systems. *Phil. Trans. R. Soc. A* **366**(1881), 3759–3767 (October 2008)
35. Ryan, P.Y.A., Bismark, D., Heather, J., Schneider, S., Xia, Z.: Prêt à Voter: A voter-verifiable voting system. *IEEE Transactions on Information Forensics and Security* **4**(4), 662–673 (2009)
36. Sarwate, A.D., Checkoway, S., Shacham, H.: Risk-limiting audits and the margin of victory in nonplurality elections. *Statistics, Politics and Policy* **4**(1), 29–64 (2013)
37. ScannerOne: Kodak i5600. <http://www.scannerone.com/product/KOD-i5600.html>
38. Stamm, M.C., Liu, K.R.: Forensic detection of image manipulation using statistical intrinsic fingerprints. *IEEE Transactions on Information Forensics and Security* **5**(3), 492–506 (2010)
39. Stark, P.: Conservative statistical post-election audits. *Ann. Appl. Stat.* **2**(2), 550–581 (2008)
40. Stark, P.: Super-simple simultaneous single-ballot risk-limiting audits. In: 2010 Electronic Voting Technology Workshop / Workshop on Trustworthy Elections (EVT/WOTE ’10). USENIX (2010)
41. Stark, P.B., Teague, V., Essex, A.: Verifiable European elections: Risk-limiting audits for D’Hondt and its relatives. *USENIX Journal of Election Technology and Systems (JETS)* **1**, 18–39 (2014)
42. Unisyn Voting Solutions: OpenElect OCS Auditor. <https://unisynvoting.com/openelect-ocs/>
43. U.S. Election Assistance Commission: Certificate of conformance: ClearVote 1.5. <https://www.eac.gov/file.aspx?A=zgte4IhsHz%2bswC%2bW4LO6PxIVssxXBbhvZiSd5BGbbs%3d> (2019)
44. Verified Voting Foundation: The Verifier: Polling place equipment (2019), <https://www.verifiedvoting.org/verifier/>