AN OPEN LETTER TO ATTORNEY GENERAL YOST AND OHIO ELECTED REPRESENTATIVES ON ELECTION INTEGRITY IN ANTICIPATION OF THE 2024 GENERAL ELECTION

We, a collective of registered voters in the State of Ohio, hereby invoke our constitutional and natural rights under the United States Constitution, including but not limited to our right under the First Amendment to peaceably assemble and to petition the Government for a redress of grievances. Further, we invoke the Ohio Constitution, Article I, Section 11, which states that every Ohio citizen may "freely speak, write, and publish his sentiments on all subjects … and no law shall be passed to restrain or abridge the liberty of speech, or of the press." As Americans and as Ohioans, we hereby invoke these rights and petition the Attorney General of the State of Ohio to perform his official duties of office as specified in Revised Code Chapter 109 and in § 1345.06 to promptly investigate and act on the serious issues raised below. In addition, we call upon the Ohio legislature and all other state and local government officials who bear, in any capacity, the responsibility for administering elections or for enacting the legal framework of elections, to take immediate steps to prohibit the use of electronic voting systems, machines and equipment (hereafter voting systems) in this State for any elections, particularly while these matters are under review by the Attorney General.

Attorney General Yost, we hereby notify you, as the Law Enforcement Officer in Chief of the State of Ohio, of our grave concerns regarding what we believe to be a failure to protect the constitutional rights of Ohio voters to have their votes transparently counted and accounted for. This failure is – in our view – multifaceted and we believe it to be systemic in nature, such that no one single legal theory can address the significant issues we have identified in the Secretary of State's certification process as set forth in Ohio law and in actual practice. However, our primary concern is for the serious issues we have identified with these voting systems to be investigated as a consumer protection issue and as a certification compliance issue. Consequently, we demand a full, immediate, and transparent investigation and legal review of the issues we have identified and raised here as Ohio citizens and voters.

Unless and until these issues are completely and transparently addressed, we petition that the Ohio Secretary of State and county Boards of Elections should not be permitted to allow or accept voting or vote tabulation done by any voting system which relies on electronic devices in whole or in part. In other words, we respectfully demand that all voters cast their vote by transparently auditable paper ballot, for the reasons provided below.

ISSUE I: WHETHER THERE HAS BEEN A FAILURE TO CERTIFY VOTING MACHINES UNDER THE STANDARDS OHIO IMPLEMENTED UNDER THE REVISED CODE PURSUANT TO THE HELP AMERICA VOTE ACT

Article V, Section 2 of the Ohio Constitution, which was adopted in 1851, requires that elections are to be conducted by manner of casting ballots. This section of the Ohio Constitution captures the general sentiment that, at that time, ballots were cast anonymously using paper. It follows

that any technology taking the place of paper ballots should not diminish the ability of voters to be able to see and observe the collection and counting of votes.

The Help America Vote Act (HAVA) was intended to federalize elections by encouraging a transition to voting systems which were claimed to be more reliable but relied upon programmable machines to perform the essential functions of tallying and reporting vote totals. In an apparent attempt to allay concerns that such machine processes are not transparent, HAVA Title III provides for minimum "voting system standards." 52 U.S.C. § 21081. HAVA also established the Election Assistance Commission (EAC) to administer a certification program for testing and certifying voting systems. Despite acknowledging that its testing standards from 2005 are out of date, the EAC continues to assert that voting systems certified under the 2005 testing standards are not going to be decertified regardless of the EAC's shift to an allegedly higher testing standard (and notwithstanding the fact that these 2005 standards do not require a detailed source code review).[1] Equally concerning, the Scope of Certification for EAC Certificates of Conformance provides disclaimers as to whether the certifications meet HAVA requirements or serve as a warranty of the voting system or any of its components.[2]

Ohio law has specific testing requirements which provide that, as a condition of continued certification and use, any voting machine, tabulation device, or automatic tabulating equipment must meet the 2002 voting standards of the Federal Election Commission or the voluntary voting system guidelines most recently adopted by the EAC. This requirement does not apply to any equipment not certified by the EAC as part of its testing and certification program. Consequently, in order to be properly certified for use in this State, Ohio voting systems, machines or equipment subject to EAC testing and certification must be certified by the EAC under its latest testing standards from 2021 or under the Federal Election Commission (FEC) guidelines from 2002. O.R.C. § 3506.05(h)(4)(a) and (b); see also 52 U.S.C. § 21081(a)(5). **However, all of Ohio's currently certified voting systems are only certified by the EAC under these outdated 2005 standards, and none were certified by the EAC under the 2002 FEC Guidelines**.[3] Further, we have been unable to locate information detailing the actual testing of voting systems by the EAC using accredited test labs after 2017, as required under HAVA. 52 U.S.C. § 20971.

This begs the question of what oversight the Ohio Board of Law Machine Examiners (BOLME), or county Boards of Elections (all of whom are appointed by the Ohio Secretary of State under O.R.C. § 3501.06) exercised when examining the voting systems listed as certified by the Secretary of State as of October 2023. Upon examining the little information publicly available, the BOLME follows the requirements set forth in Ohio Administrative Code 111:3-2-06 and Secretary of State Directives 2011-45 and 2012-34, which are presented in a checklist entitled "Ohio Voting System Requirements Matrix" (Matrix). The Matrix has one criterion for checking that the equipment was certified by the EAC and meets its standards, as well as simple operational, logic and accuracy, and external security checks. The Matrix also requires discussion and demonstration of backup memory and physical audit trail, *if any,* and the ability to manually enter data, clear tabulating memory, and re-run ballots. There is no stated requirement for an eyes-on examination of the source code, despite the recent update to the Revised Code in §

3506.14, which expressly requires only logic and accuracy testing.[4] As discussed below, logic and accuracy testing is not sufficient to detect issues with source code.

The Matrix also requires warranty information for the equipment pursuant to O.R.C. § 3506.10 to "correctly, accurately, and continuously register and record every vote cast" and to be free from "defects in workership and materials for a period of five years." However, the State of Ohio's requirements contract for voting systems purchases effective from November 21, 2018 through June 30, 2023 contains "Equipment and Software Warrantees" which do not address the accuracy of voting systems according to any specific technical standard, and *disclaims any implied warranties of merchantability or fitness for a particular purpose*. We find this waiver extremely concerning, considering that the Texas Secretary of State refused to certify the Dominion Democracy Suite 5.5-A voting system in 2019 because the examiners' reports raised concerns as to whether the system was "suitable for its intended purpose."[5] Why has this common law warranty been waived in Ohio, and on whose authority was this done?

Instead, according to the requirements contract, voting systems in Ohio are only warranted against "fail[ure] to perform in accordance with [their] documentation in all material respects" and against defective material and workmanship.[6] We find it extremely concerning that the State of Ohio would insert such minimal warrantees in a contract for the purchase of voting systems, without such "documentation" being transparent to the voters who are apparently expected to use and trust these systems, without question. Furthermore, it is the voters of this State who are the consumers of these voting systems which the State has approved for purchase on their behalf.

We also do not find it appropriate in terms of complying with Revised Code § 3506.06(H)(1) that guidelines "shall" require vendors of software developers to place a copy of all source code "in escrow with an independent escrow agent," where such independent agent may be subject to control from outside the United States. For example, the ES&S October 2018 quote to Ohio lists Iron Mountain Intellectual Property Management, Inc., which was recently purchased by NCC (a multinational corporation headquartered in the United Kingdom).[7] Moreover, although Dominion did not name their escrow company in their quote submitted on October 2018, they have historically represented that they also use the NCC Group as their escrow agent.[8] Any appearance of foreign influence is unacceptable and undermines the rationale for holding source code in escrow.

Consequently, we demand an immediate investigation into whether Ohio has failed to certify voting systems currently in use according to the technical requirements set forth in the Revised Code §§ 3506.05 and 3506.10, and the reasons for any failure to comply with Ohio's technical certification standards.

ISSUE 2: WHETHER THE STATE HAS BEEN ON NOTICE SINCE AT LEAST 2007 THAT THERE ARE FUNDAMENTAL DESIGN FLAWS WITH THESE VOTING SYSTEMS

The State of Ohio acting as *parens patriae* has responsibility for ensuring that these voting systems are warranted to "correctly, accurately, and continuously register and record every vote

cast." O.R.C. § 3506.10. However, even assuming that these voting systems were potentially capable of meeting this standard, does the State of Ohio have the ability to verify that these systems are compliant with this specific technical standard, or indeed even whether these systems are being required to record and accurately tally every *lawful* vote? Are these systems fundamentally flawed? We are seeing growing evidence that there are persistent, fundamental problems with these voting systems. The electronic voting system infrastructure is alleged to have been effectively outsourced to "a handful of corporations that operate in the shadows, with little oversight or accountability."[9] Allegations have been raised that the systems within this small market may be fundamentally compromised to the extent that an ordinary audit would not detect any latent defect in the proprietary source code, such as with a "cipher trapdoor" in the case of Dominion.[10]

Certainly, there have been longstanding criticisms of the lack of transparency of these systems as well as the small, private market in which the manufacturers of voting systems operate. For example, in the early 2000s, King County Washington resident Bev Harris raised the alarm about leaving vote tabulation in the hands machines built by private corporations.[11] Ms. Harris submitted in her book *Black Box Voting: Ballot Tampering in the 21st Century* that, with electronic voting systems, a compromised system would only require "an insider, someone with access, to plant malicious code without getting caught."[12] Harris also identified vetting issues with key programmers of source code. For example, she alleged that Jeffrey Dean, a convicted felon, worked on the computerized election system which "came to dominate the US absentee voting market.".[13] She further alleged that Dean was subsequently a Diebold senior programmer for the Global Election Management Systems (GEMS) server (Diebold central tabulating software), and traced the implementation of multiple sets of books on the system to this period of time.[14]

Ms. Harris' research on the history of Diebold Election Systems Inc., which has been owned by both ES&S and Dominion (two of the largest vendors in this State), is concerning. She reports that the CEO of Diebold, Inc. infamously wrote a letter in 2003 in the context of a Republican fundraiser that said, "I am committed to helping Ohio deliver its electoral votes to the president next year."[15] ES&S acquired Premier Election Solutions (formerly known as Diebold Election Systems) in 2009, and the DOJ subsequently launched an investigation into the transaction on antitrust grounds.[16] Nine state Attorneys General joined the suit, asserting that the merger was harmful to competition.[17] The DOJ complaint alleged that the acquisition substantially reduced competition as it **combined the two largest providers of systems used to tally votes in federal, state, and local elections in the United States**.[18] As a result of a DOJ antitrust suit, the Premier/Diebold assets were sold to Dominion.[19]

Ms. Harris further alleges that two of Diebold's programmers, Talbot Iredale and Guy Lancaster, had "been designing and programming election machines for Diebold Election Systems Inc. and its predecessors since 1988" and developed the ES-2000 optical scan voting system used in a majority of states.[20] Ms. Harris reported that Diebold's history at this time was linked to the three founders of North American Professional Technologies, Macrotrends International Ventures, Inc. and Global Election Systems: Norton Cooper, Charles Hong Lee, and Michael K. Graye –each of

whom had outstanding civil liabilities and/or criminal histories.[21] Ms. Harris' investigation into the complex ownership structure of ES&S, the largest voting machine vendor in this State, showed a link to Peter Kiewit Sons' Inc., who had been tied to bid-rigging cases in as many as 11 states and two countries.[22]

Another allegation, by Patrick Byrne, points to complex connections between these main players and Smartmatic International, particularly the assertion that code from Smartmatic systems was developed in Venezuela and, "[t]hrough a series of licensing agreements, bankruptcies, and corporate mergers and acquisitions, … code ended up in various US election systems (e.g., Dominion, ES&S) which (branding aside) still derive from Smartmatic (a.k.a. Sequoia). Thus, they brought to US elections not only the generous functionalities permitting manipulation by administrators, but porous security, extending such powers to those abroad."[23]

Whistleblower testimony indicates that Ohio may have been a target of coding manipulation starting in the early 2000s. Clinton Curtis, a computer programmer who worked for Yang Enterprises in Oviedo, Florida, testified before Congress in December 2004 that he was asked to insert fraudulent code into touch-screen voting systems.[24] He testified that he wrote code to rig votes to show a 51%-49% outcome in the 2000 elections, but the rigging would be undetectable as part of the source code.[25] The programming he was requested to develop would enable a user to press hidden buttons to flip the vote in the machine without requiring any plug-ins, and would be undetectable, even if the source code was seen.[26] Curtis testified before Congress that he would not have been able to protect the Ohio elections against this kind of manipulation; programmers would have to look at the source code to search for the improper code inserted in the software.[27]

Mr. Curtis' opinion before Congress, under oath, was that the Ohio presidential election was hacked because the exit polling data was significantly different from the published results of the election. Curtis testified that one might be able, depending on the sophistication of the programming, to identify the tampering after the fact; however, some code could "eat itself" as it was being executed. Curtis additionally testified that inserting bad code into a central tabulation machine could affect the tabulation of tens of thousands of votes by flipping them. Furthermore, Curtis attests that he could program the central tabulator and individual machines to match results by talking to each other.[28] In other words, as early as 2004, Ohio was placed on notice by whistleblower testimony that it was possible to manipulate source code in tabulating machines and to manipulate results without such manipulation being easily detectable. It has been reported that Mr. Curtis shortly thereafter passed a lie detector test administered by the retired chief polygraph operator for the Florida Department of Law Enforcement.[29]

On March 28, 2023, Mr. Curtis was before the Shasta County Board of Supervisors and reiterated that the fundamental problem had not changed; there was corporate control of the elections with the software, source code, and system blueprints not open to external review.[30] His opinion was based on his experience with coding at the assembly level of machines, which, he pointed out, has not changed over time.[31] Curtis stated that the process is compromised such that we cannot know (verify) the actual winner of an election.[32]

It is our understanding that Ohio has already had some expert review of voting systems which echo these fundamental concerns about how voting systems work. In December 2007, Everest issued its final report on the evaluation and validation of election-related equipment, standards, and testing. This report was initiated and released by the Ohio Secretary of State and was conducted by teams from Pennsylvania State University, the University of Pennsylvania, and Web Wise Security, Inc. The teams were provided the source code, software, and election equipment for the majority of systems used in Ohio.[33] According to the Executive Summary, the following conclusions were reached:

- **Insufficient Security** - The systems uniformly failed to adequately address important threats against election data and processes. Central among these is a failure to adequately defend an election from insiders, to prevent virally infected software from compromising entire precincts and counties, and to ensure cast votes are appropriately protected and accurately counted.

- **Improper Use or Implementation of Security Technology** - A root cause of the failures present in the studied systems is the pervasive mis-application of security technology. Failure to follow standard and well-known practices for the use of cryptography, key and password management, and security hardware seriously undermine the protections provided. In several important cases, the misapplication of commonly accepted principles renders the security technology of no use whatsoever.

- **Auditing** - All of the systems exhibited a visible lack of trustworthy auditing capability. In all systems, the logs of election practices were commonly forgeable or erasable by the principals who they were intended to be monitoring. The impact of the lack of secure auditing is that it is difficult to know when an attack occurs, or to know how to isolate or recover from it when it is detected.

- **Software Maintenance** - The software maintenance practices of the studied systems are deeply flawed. This has led to fragile software in which exploitable crashes, lockups, and failures are common in normal use. Such software instability is likely to increase over time, and may lead to highly insecure and unreliable elections.

The report added that, in many cases, they could not identify any practical procedures that adequately addressed the security issues present. In addition, the report states that "[t]he security of the studied election systems is **crippled by flaws in its design and implementation**. Therefore, after an extensive analysis, the **teams unanimously believe that such flaws mandate fundamental and broad reengineering before the technical protections can approach the goal of guaranteeing trustworthy elections**."[34] Significantly, the report states that an attacker involved in the development or production of the software and hardware for the election system has ample opportunity for subverting the system, including, for example, inserting exploitable vulnerabilities, back doors, or malicious code into the system.[35] Moreover, some attacks are undetectable no matter what practices are followed, which casts doubt on the validity of an election.[36]

Although the controversy over electronic voting systems has been ongoing since the early 2000s, as evidenced by Bev Harris' 2003 book *Black Box Voting*, it would appear that issues touching on the reliability of these voting systems since that time, are mostly re-raised by partisan groups whose preferred candidate lost during each election cycle. We refer, for example, to the

Democrat party questioning results from the 2016 election, who did not question the results from 2020, and vice versa. We particularly question those in this State who think that, because they are registered Republican and Ohio is seen by many as a "red" state, there is no need to assess the accuracy and reliability of voting systems here, because their chosen candidate(s) may have won in 2020 and 2022. We do not see this as a partisan issue but a fundamental civil rights issue. Without transparency, no voter can be assured that his or her vote actually counts.

Professor Alex Halderman, a prominent cyber security expert, has consistently attempted to expose such fundamental concerns for at least the past 8 years. He testified before the Senate Select Committee on Intelligence in 2017 that the only reason no one was able to prove that voting systems were hacked in 2016 is because no one allowed anyone to actually check.[37] Professor Halderman also has advocated for routine audits of results by using paper ballots.[38] The concern after 2016 was such that Senator Wyden of Oregon sent detailed questionnaires in 2019 to manufacturers to get more information on security but received little in response.[39] He said: "The market is broken… Markets work well when you have tough standards, when you have real regulations and vigorous oversight. And here you have none of that."[40] As will be discussed below, Professor Halderman has recently contributed as an expert witness on these concerns.

ISSUE 3: WHETHER NEW CONCERNS REGARDING THE FUNDAMENTAL SUSCEPTIBILIY OF VOTING SYSTEMS TO MANIPULATION REQUIRES CORRECTIVE ACTION

As we have already pointed out, the fundamental concerns raised above have not gone away. The problem with these voting systems is fundamental to their design, according to the Everest report. In March 2019, researchers associated with the University of Melbourne and the Open Privacy Research Society conducted a review of the electronic voting system used in Swiss elections.[41] They found that the "SwissPost-Scytl mixnet uses a trapdoor commitment scheme, which allows an authority who knows the trapdoor values to generate a shuffle proof transcript that passes verification but actually alters votes."[42] The question is whether such concerns were ever specifically addressed by the United States or individual states in recent years, when there have been legitimate and ongoing questions about these systems.

Tore Maras, a CIA contractor turned whistleblower with formal training in algorithmic aspects of machine learning and predictive analytics, two decades of experience in mathematical modeling and pattern analysis, and an amateur network tracer and cryptographer, also raised the alarm in 2019. She published an article on concerns of election fraud raised in the State of Kentucky. As a result of her investigation, she identified and demonstrated with proofs that the machines were compromised.[43] Her ultimate conclusion was that "[w]e should not be allowing these companies to facilitate our elections because their programming is not universally verifiable. Verifiability is another way of being able to prove something with math proofs."[44] She also determined that it was "obvious" that "NO ONE bothered to look into it [and it] took a week of casual brush-up and crunching some proofs with what she had" to reach this determination.[45] She concluded that "this illustrates complacency or severe negligence by our government in respect to protecting the

integrity of our vote. This has been going on for almost a decade and that speaks volumes."[46] Ms. Maras subsequently drafted a sworn declaration discussing her proofs which has been introduced into multiple lawsuits, including *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020)). To date, no one has successfully disproved the substance of her claims in any forum.

In addition, there have been significant developments in the case of *Curling v. Raffensberger* (Case No. 1:2017-cv-02989, N.D. Ga). This case has been allowed to proceed to trial in large part due to the expert opinion, which has recently been released to the public, of Professor Alex Halderman. In this case, the issue pertains to whether Georgia's statewide voting system, as currently designed and implemented, is so deficient that it unconstitutionally burdens the Plaintiffs' First and Fourteenth Amendment rights to cast effective votes that are accurately counted.[47]

Judge Totenberg noted that Professor Halderman's report findings were consistent with a "broad consensus" among the nation's cybersecurity experts that electronic voting systems are susceptible to malware.[48] According to the Court, which assessed the Dominion BMD system implemented in 2019 (which is also certified for use in this State), Halderman reached the following major findings:

> **The ICX BMDs are not sufficiently secured** against technical compromise to withstand vote-altering attacks by bad actors who are likely to attack future elections in Georgia. . .
>
> The ICX **BMDs can be compromised to the same extent and as or more easily than the AccuVote TS and TS-X DREs** they replaced. . . .
>
> Despite the addition of a paper trail, ICX **malware can still change individual votes and most election outcomes without detection** . . . Although outcome-changing fraud conducted in this manner could be detected by a risk-limiting audit, Georgia requires a risk-limiting audit of only one contest every two years, so the vast majority of elections and contests have no such assurance. And even the most robust risk-limiting audit can only assess an election outcome; it cannot evaluate whether individual votes counted as intended. . . .
>
> The **ICX's vulnerabilities also make it possible for an attacker to compromise the auditability of the ballots**, by altering both the QR codes and the human readable text. Such cheating could not be detected by a [risk-limiting audit] or a hand count, since all records of the voter's intent would be wrong. . . .
>
> **Using vulnerable ICX BMDs for all in-person voters, as Georgia does, greatly magnifies the security risks** compared to jurisdictions that use hand-marked paper ballots but provide BMDs to voter upon request. . . .
>
> The critical vulnerabilities in the ICX — and the wide variety of lesser but still serious security issues — indicate that **it was developed without sufficient attention to security**

> during design, software engineering, and testing. . . . [I]t would be extremely difficult to retrofit security into a system that was not initially produced with such a process.[49]

It is also noteworthy that Professor Halderman stated in his report, released in the *Curling* case, that there were a lot of things he could not do as part of his forensic analysis. He commented that Ohio used Open Ended Vulnerability Testing (OEVT) (presumably for the Everest report), which essentially means a hacker looks for ways to compromise the system.[50] Given that each system has over a million lines of code,[51] there are limitations to what can be uncovered using this approach. Specifically, Professor Halderman stated in his report:

> It is highly dependent on the skill, resources, and experience of the testers, and also on good luck. I was fortunate that many of the observations that I decided to pursue through detailed testing proved to be productive, but there were many other observations that I decided not to pursue, and I almost certainly overlooked clues to other important weaknesses. Due to time and resource constraints, once I found one way to accomplish an adversarial objective (e.g., installing malware remotely), I usually moved on to another goal, rather than attempting to find all ways of accomplishing it. For these reasons, I stress that while my methodology is effective for discovering and proving the existence of security problems, the vulnerabilities I uncovered are almost certainly not the only such problems affecting the equipment I studied.[52]

As mentioned above, Ms. Maras has also provided evidence on systemic vulnerabilities in the 2020 election cycle. She explained that in using Commercial Off The Shelf (COTS) operating systems such as Windows Operating Systems, election machine vendors such as Dominion, ES&S, Hart Intercivic, Smartmatic and others create problems in that "such manufacturing for COTS have been outsourced to China which if implemented in our Election Machines make us vulnerable to BLACK BOX antics and backdoors due to hardware changes that can go undetected."[53]

In her declaration, Ms. Maras outlines the process of how a ballot is cast and then processed in a voting system. She specifically identifies the point of vulnerability in the source code when votes are encrypted and decrypted. In the third step, the vote is shuffled or mixed: "the software takes all the votes, literally mixes them … and then re-encrypts them. This is where if ONE had the commitment key – TRAPDOOR KEY – one would be able to see the parameters of the algorithm deployed as the votes go into this mixing phase, and how [the] algorithm redistributes the votes."[54] She adds that "when this mixing/shuffling occurs, then one doesn't have the ability to know that vote coming out on the other end is actually their vote; therefore, ZERO integrity of the votes when mixed."[55] She states that within a trapdoor, an algorithm can "move the goal posts" in elections without being detected, as shown by her mathematical proof.[56] Essentially, she states that no one can see what is going on during the shuffling, thus, even if algorithms or manual scripts were deployed to fractionalize or distribute pooled votes to achieve the outcome desired, there is no way to prove it is being done: thus, the results are unverifiable.[57]

We note that, at the *Curling* trial, Professor Halderman provided a compelling demonstration of the defective design of the Dominion BMD System by using a pen to, within minutes, facilitate access to a number of administrative applications in the system, such as the file manager, which

would allow him to change or delete files, or the settings, which allow not only settings changes but also to add or remove software on the device.[58]

The implications of this evidence are significant and simultaneously horrifying. Even if these machines were not purposely designed to be so easily manipulated, they present issues as to whether these voting systems are fundamentally defective, as suggested by the 2007 Everest study and the ongoing cybersecurity concerns. No average Ohio voter would have the knowledge or expertise to make such cybersecurity assessments, and we must rely on neutral experts like Dr. Halderman to alert us to system vulnerabilities which could compromise an election and raise again the problem of lack of verifiability of results. Further, the obligation is on the State, not the voters, to show that these systems meet legal and technical standards, and we now demand immediate action to protect the interests of Ohio voters.

There is an unavoidable paradox at the heart of this matter: no voter can see or verify the votes as tabulated and is expected to simply defer to what are purported to be trusted systems. However, no one has been transparent as the source code remains shrouded in secrecy, despite the token gesture under Ohio law to hold source code in escrow to be accessed by the Secretary of State. As we have pointed out, the manner in which this safeguard has been used in practice raises common sense concerns which do not require special technical expertise to appreciate. Who, we ask, is capable of even verifying that the source code provided in escrow is that on the voting systems in each precinct, or that the source code present does not have the defects identified above? Who has subjected these systems to the extensive testing and analysis recommended by Ms. Maras and Professor Halderman?

If the State's response is that the EAC is well suited to perform these assessments and that Ohio can rely on the safety and accuracy of their certification process, we reject that premise first because Ohio is to certify under its own standards, and second because the EAC has also not been sufficiently transparent or effective to identify or flag this glaring issue. We now address the issues we have found with the operation of the EAC certification process.

ISSUE 4: WHETHER OHIO SHOULD BE CONCERNED BY BROADER SYSTEMIC ISSUES INVOLVING TECHNICAL REVIEW AND CERTIFICATION WITH THE EAC

Ohio law requires Federal certification for voting systems. O.R.C. § 3506.05(h)(4). Consequently, this State requires that its voting systems are tested by a federally accredited testing authority that is compliant with EAC standards. 52 U.S.C. §§ 20971, 21081. As discussed above, the EAC is currently relying on technical standards from 2005 to certify machines, which does not rise to Ohio's standard of using the "most recently adopted" standards from the EAC. O.R.C. § 3506.05. However, this is not the full extent of the problem when it comes to reliance on the EAC as a trusted certifying authority.

As an initial example, even if Ohio were to use the EAC's most recent version of the VVSG (VVSG 2.0, approved in 2021) to evaluate voting systems to be used in Ohio, we believe the entire test lab accreditation and certification system is seriously flawed and could be vulnerable to regulatory capture. For example, the EAC was subjected to a federal lawsuit by a member of its Board of Advisors after unilaterally lowering the standards contemplated in the version of

VVSG 2.0 released for public comment in March 2020.[59] According to the Complaint, the EAC relies upon the Standards Board, the Board of Advisors, and the Technical Guidelines Development Committee (TGDC) to create the VVSG.[60] The National Institute of Standards and Technology (NIST) chairs the TGDC and receives funding from the EAC to support the development of the VVSG. According to the complaint, the EAC Board of Advisors voted to approve the VVSG 2.0 on July 31, 2020, but subsequently met privately with voting machine vendors on a weekly basis from July through August 2020.[61] The Complaint alleges that changes were made to the VVSG 2.0 and that the version was presented to the Board of Advisors for approval in early 2021 without facilitating public comment or providing a summary of the changes to the Board of Advisors until nine days before the vote.[62] One of the noteworthy changes was the reversal of the proposed requirement to ban wireless networking devices in voting machines.[63] Another change was the limitation to voter-facing devices of the logging requirements for backend voting systems to record external connections or disconnections during the activated voting state.[64]

The Gateway Pundit in 2021 described the EAC as "an understaffed tiny federal agency" using two private labs responsible for certification of the nation's voting systems.[65] It raised the alarm at that time that one of its chief employees, Jennifer Bowers, was a former executive of Dominion Voting Systems for 10 years and was active in implementing Dominion Systems in a number of states.[66] On the operational side, the claim by Don Palmer on December 16, 2020 that it had two accredited testing firms for testing (using the VVSG standards) was in fact not true, and the Gateway Pundit found that the labs had not been accredited for some time.[67] When this issue was brought before the EAC, they updated their website to state the labs were accredited.[68] However, when NIST (who evaluates test labs for EAC accreditation under § 231 of HAVA) was asked via FOIA request for the documentation showing calibrated equipment lists and any attachments for the two allegedly EAC accredited labs (ProV&V Inc. and SLI) between 2016 and 2021, FOIA Officer Catherine Fletcher stated that there were no responsive documents.[69]

Thus, although the EAC conceded that a lack of lab accreditation occurred due to "administrative error" from 2017 to 2019,[70] we question whether *any* compliant lab accreditation took place during this time period or that the EAC had the capacity to lawfully certify voting systems without a duly accredited lab under the requirements of HAVA § 231 and the EAC Voting System Test Laboratory Program Manual (VSTLPM).[71] We were, in fact, unable to obtain EAC certifications for voting systems for the period running up to the 2020 elections. The EAC has now announced that only one voting system so far, as of January 2024, is being considered under VVSG 2.0 after accrediting two test labs in November and December 2022.[72] This does not appear to be consistent with the EAC's stated adoption of VVSG 2.0 as a "national security imperative."[73]

Our position is that the State of Ohio must inquire into whether the EAC had or has the legal capacity to certify any machine if it is held to comply with its own accreditation and certification policies, procedures, and HAVA itself. This question is particularly relevant for those voting systems which have been held out as EAC certified and eligible for certification in Ohio with the Secretary of State. This issue cannot be glossed over, as the role of these labs in evaluating

cybersecurity matters for these machines is clear, as provided in the VSTLPM and Ms. Maras' declaration.[74] Specifically, Ms. Maras states that it is the role of VSTLs to ensure that there are no foreign interference/bad actors accessing the tally data via backdoors in equipment software.[75]

Further, as illustrated in the *Curling* case with Professor Halderman's testimony at trial, a "serious security problem" with the federal certification process is the fact that EAC approval must be obtained for "any changes to election system software, including Windows updates."[76] It appears, given the evidence from Ms. Maras and Professor Halderman, that the frequent security updates required of COTS proprietary software would make the job of keeping certifications up to date under the EAC process and of coordinating with all voting system vendors and states extremely difficult. Moreover, the EAC's website does not reflect that it is staying current with these updates in certifying voting systems as often as these updates occur. Given the lack of evidence that it had properly accredited third party testing labs for a significant period of time prior to or after the 2020 elections, the EAC does not appear to be in a position to keep up with this kind of compliance. Consequently, we do not believe it appropriate or acceptable for Ohio to place its trust in the EAC certification mechanism.

CONCLUSION:

All voters have a right to expect transparent elections and transparent governance. We expect our constitutional right to have a voice in federal and state elections to be honored. The question before us is: what efforts have been made by the State of Ohio, or by the EAC for that matter, to assure voters that their lawful votes are accurately counted and not subject to manipulation of proprietary source code during the tabulation process? The State of Ohio requires that voting systems are not acceptable for use if, pursuant to O.R.C. § 3506.10, they cannot "correctly, accurately, and continuously register and record every vote cast, and further [guarantee] those machines against defects in workership and materials for a period of five years from the date of their acquisition." As a result, Ohio voters are unable to benefit from the purchase of these voting systems.

As we have discussed above, these voting systems: 1) are products which are mandated by state law to perform at a verifiable level of accuracy for the benefit of Ohio voters, and 2) must be certified according to specific technical standards at both federal and state level in order to be used in State elections. We believe the implications of failing to meet one or both of these requirements are sufficiently serious that they demand your immediate attention and action. Accordingly, we respectfully request the following:

1. That the Attorney General **immediately** commence an investigation pursuant to O.R.C. § 1345.06 based upon the issues discussed above, make his findings publicly available, and pursue any and all available legal remedies on behalf of Ohio voters and taxpayers.
2. That the Attorney General **immediately** perform a full legal review as to whether HAVA actually *requires* the full implementation and use of electronic voting systems for all Ohio voters, or whether it may be implemented on a limited basis as an accommodation for disabled voters by providing one such system at each polling place.

3. That the Attorney General **immediately** provide a full legal review on the issue of whether the current electronic voting systems recognized by the Secretary of State for certification are in full compliance with Ohio law and do in fact meet the legal and technical requirements of certification.
4. That the Ohio legislature enact emergency legislation prohibiting any county Board of Elections from using these electronic voting systems for the reasons provided above, and that the Secretary of State and all Boards of Elections take all legal and available steps to cease and desist from using these electronic voting systems due to the issues discussed above. We intend to share this information in our communities so that the registered voters in Ohio can hold all of their elected representatives responsible for acting to correct this serious security issue before any further harm is caused.
5. That our local boards of elections act to **immediately** move to counterfeit-proof, serialized paper ballots and away from electronic voting systems for the 2024 elections, for the reasons provided above.

We note that the Ohio primaries take place on March 19, 2024. We expect that all the above-mentioned elected officials will address these issues in the urgent manner they deserve prior to the primary, and we will document the progress made on these matters both before and after the primary elections. We expect swift, transparent action on the part of State and local government to revert to the exclusive use of counterfeit-proof, serialized paper ballots for fair, verifiable, and accurate election results in 2024 and in the future.

We will consider all lawful courses of action, including but not limited to public exposure of these issues and of the politicians who knowingly refuse to address these issues, to enforce our right to transparent and secure elections.

Please see the attached signatures of Ohio voters in full agreement with this voter-led initiative.

---

[1] https://www.eac.gov/voting-equipment/certified-voting-systems; https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines (last accessed February 10, 2024); https://www.transparentelectionsnc.org/source-code-review-nc-electronic-voting-system, Expert Comment 1 ("The EAC testing program for VVSG 1.0 does not require a detailed source code review." (Last accessed February 10, 2024)

[2] See for example, certs for Voting Systems used in Ohio (such as Dominion Suite 5.5 and 5.5D and ES&S EVS versions 6.2.0.0, 6.1.1.0, 6.0.2.0, and 6.0.4.0), link to certs at: https://www.eac.gov/voting-equipment/certified-voting-systems (last accessed February 10, 2024). Importantly, the EAC acknowledged that the new standards include "desperately needed" improvements pertaining to multiple issues including cybersecurity. "As elections are decentralized throughout the country, the VVSG [the updated standards from 2021] are the only set of uniform specifications and requirements against which voting systems can be tested to determine if the voting systems meet required standards. Some factors examined under these tests include basic functionality, accessibility, accuracy, reliability, and security capabilities." https://www.eac.gov/news/2021/02/10/us-election-assistance-commission-adopts-new-voluntary-voting-system-guidelines-20 (last accessed February 10, 2024).

[3] https://www.ohiosos.gov/globalassets/elections/bvme/certifiedvotingsystemsohio_10-06-23.pdf; https://www.eac.gov/voting-equipment/certified-voting-systems (last accessed February 10, 2024).

[4] According to Arnold Urken, founder of the first voting machine testing lab, eyes-on examination of the source code "should be mandatory if certification is to mean anything." See Bev Harris, *Black Box Voting: Ballot-Tampering in the 21st Century* at 58.

[5] Texas Secretary of State, Voting System Examination Dominion Voting Systems Democracy Suite 5.5-A, November 4, 2019, at https://www.sos.texas.gov/elections/forms/sysexam/oct2019-pinney.pdf (Last accessed February 10, 2024).

[6] Contract No. OT902619, Mandatory Use Contract for Voting Systems, page 7.
[7] ES&S Quotation for ITB #OT902619 at 57; see https://www.escrowcompany.co/news/ncc-group-acquires-iron-mountain-escrow/ (Last accessed February 10, 2024).
[8] Dominion quotation for ITB #OT902619; New Mexico Secretary of State, Report on Dominion Voting System Democracy Suite 4.14 software at https://verifiedvoting.org/wp-content/uploads/2020/08/NM-Dominion-Democracy-Suite.pdf (Last accessed February 10, 2024).
[9] https://www.electiondefense.org/how-to-rig-an-election (Last accessed February 10, 2024).
[10] See, for example, Tore Maras, "Dominion's Own FROG Destroys Their Claim," at https://toresays.com/2021/02/11/dominions-own-frog-destroys-their-claim/ (last accessed February 10, 2024).
[11] https://www.seattleweekly.com/news/once-a-liberal-darling-bev-harris-still-thinks-the-elections-are-rigged/ (last accessed February 10, 2024).
[12] Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century,* at 45. https://blackboxvoting.org/black-box-voting-book/ (Last accessed February 10, 2024).
[13] https://www.opednews.com/articles/1/Two-convicted-felons-invol-by-Bev-Harris-101013-716.html (Last accessed February 10, 2024).
[14] *See* http://www.ejfi.org/Voting/Voting-37.htm (Last accessed February 10, 2024). It is also noteworthy that the publicly accessible GEMS files have been evaluated and that the "GEMS architecture fail[ed] to conform to fundamental database design principles and software industry standards for ensuring accurate data." https://www.researchgate.net/publication/254582315_GEMS_Tabulation_Database_Design_Issues_in_Relation_to_Voting_System_Certification_Standards (Last accessed February 10, 2024).
[15] Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century,* at 89. https://blackboxvoting.org/black-box-voting-book/ (Last accessed February 10, 2024).
[16] https://www.justice.gov/opa/pr/justice-department-requires-key-divestiture-election-systems-softwarepremier-election (Last accessed February 10, 2024).
[17] https://www.justice.gov/opa/pr/justice-department-requires-key-divestiture-election-systems-softwarepremier-election (Last visited January 29, 2024).
[18] https://www.justice.gov/opa/pr/justice-department-requires-key-divestiture-election-systems-softwarepremier-election (Last visited January 29, 2024) (emphasis added).
[19] https://www.justice.gov/opa/pr/justice-department-requires-key-divestiture-election-systems-softwarepremier-election (Last visited January 29, 2024).
[20] Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century,* at 90. https://blackboxvoting.org/black-box-voting-book/ (Last accessed February 10, 2024).
[21] Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century,* at 90-91. https://blackboxvoting.org/black-box-voting-book/ (Last accessed February 10, 2024).
[22] Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century,* at 74-77. https://blackboxvoting.org/black-box-voting-book/ (Last accessed February 10, 2024).
[23] Patrick Byrne, "Evidence Grows: '20 Election Was Rigged," at https://www.deepcapture.com/2020/11/election-2020-was-rigged-the-evidence/#_edn1.
[24] https://www.simpson4auditor.com/post/clinton-curtis-testimony-on-how-elections-have-been-stolen-using-algorithms-since-at-least-2000 (last accessed February 10, 2024).
[25] https://www.simpson4auditor.com/post/clinton-curtis-testimony-on-how-elections-have-been-stolen-using-algorithms-since-at-least-2000 (last accessed February 10, 2024).
[26] https://www.electionsatrisk.org/clips/computer_programmer.shtml. (last accessed February 10, 2024)
[27] https://www.simpson4auditor.com/post/clinton-curtis-testimony-on-how-elections-have-been-stolen-using-algorithms-since-at-least-2000 (last accessed February 10, 2024).
[28] https://www.simpson4auditor.com/post/clinton-curtis-testimony-on-how-elections-have-been-stolen-using-algorithms-since-at-least-2000 (last accessed February 10, 2024).
[29] https://www.electionsatrisk.org/clips/computer_programmer.shtml (last accessed February 10, 2024).
[30] Clint Curtis, Statement to Shasta County Board of Supervisors on March 28, 2023 at https://rumble.com/v2ffyh4-clint-curtis-working-for-elections-we-can-believe-in.html (Last visited accessed February 10, 2024).
[31] Clint Curtis, Statement to Shasta County Board of Supervisors on March 28, 2023 at https://rumble.com/v2ffyh4-clint-curtis-working-for-elections-we-can-believe-in.html (Last visited accessed February 10, 2024).
[32] Clint Curtis, Statement to Shasta County Board of Supervisors on March 28, 2023 at https://rumble.com/v2ffyh4-clint-curtis-working-for-elections-we-can-believe-in.html (Last visited accessed February 10, 2024).

[33] Everest: Evaluation and Validation of Election-Related Equipment, Standards, and Testing, December 7, 2007 at 3. https://nsarchive.gwu.edu/document/22371-document-06-pennsylvania-state-university (Last accessed February 10, 2024).
[34] Everest: Evaluation and Validation of Election-Related Equipment, Standards, and Testing, December 7, 2007 at 4, (emphasis added). https://nsarchive.gwu.edu/document/22371-document-06-pennsylvania-state-university (Last accessed February 10, 2024).
[35] Everest: Evaluation and Validation of Election-Related Equipment, Standards, and Testing, December 7, 2007 at 21. https://nsarchive.gwu.edu/document/22371-document-06-pennsylvania-state-university (Last accessed February 10, 2024).
[36] Everest: Evaluation and Validation of Election-Related Equipment, Standards, and Testing, December 7, 2007 at 21. https://nsarchive.gwu.edu/document/22371-document-06-pennsylvania-state-university (Last accessed February 10, 2024).
[37] Steve Friess, "Hacking the Vote: It's Easier Than You Think," at https://alumni.umich.edu/michigan-alum/hacking-the-vote/ (Last accessed February 10, 2024).
[38] Steve Friess, "Hacking the Vote: It's Easier Than You Think," at https://alumni.umich.edu/michigan-alum/hacking-the-vote/ (Last accessed February 10, 2024).
[39] ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It," at https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it; (Last accessed February 10, 2024).
[40] ProPublica, "The Market for Voting Machines Is Broken. This Company Has Thrived in It," at https://www.propublica.org/article/the-market-for-voting-machines-is-broken-this-company-has-thrived-in-it; (Last accessed February 10, 2024).
[41] https://cva.unifr.ch/content/ceci-n%E2%80%99est-pas-une-preuve-use-trapdoor-commitments-bayer-groth-proofs-and-implications (Last accessed February 10, 2024).
[42] https://cva.unifr.ch/content/ceci-n%E2%80%99est-pas-une-preuve-use-trapdoor-commitments-bayer-groth-proofs-and-implications (Last accessed February 10, 2024).
[43] Tore Maras, "Proof That Auditing Election Machines Cannot Detect Manipulation of Votes," at https://toresays.com/2019/11/22/proof-that-auditing-election-machines-cannot-detect-manipulation-of-votes/ (Last accessed February 10, 2024).
[44] Tore Maras, "Proof That Auditing Election Machines Cannot Detect Manipulation of Votes," at https://toresays.com/2019/11/22/proof-that-auditing-election-machines-cannot-detect-manipulation-of-votes/ (Last accessed February 10, 2024).
[45] Tore Maras, "Proof That Auditing Election Machines Cannot Detect Manipulation of Votes," at https://toresays.com/2019/11/22/proof-that-auditing-election-machines-cannot-detect-manipulation-of-votes/ (Last accessed February 10, 2024).
[46] Tore Maras, "Proof That Auditing Election Machines Cannot Detect Manipulation of Votes," at https://toresays.com/2019/11/22/proof-that-auditing-election-machines-cannot-detect-manipulation-of-votes/ (Last accessed February 10, 2024).
[47] See Opinion and Order, November 10, 2023, *Curling v. Raffensberger*, 1:17-cv-2989 (Atlanta Dist. Ct.) at 112.
[48] Opinion and Order, November 10, 2023, *Curling v. Raffensberger*, 1:17-cv-2989 (Atlanta Dist. Ct.) at 36.
[49] Opinion and Order, November 10, 2023, *Curling v. Raffensberger*, 1:17-cv-2989 (Atlanta Dist. Ct.) at 44.
[50] Halderman Report, *Curling v. Raffensberger*, 1:17-cv-2989 (Atlanta Dist. Ct.) at 17.
[51] See Bev Harris, *Black Box Voting: Ballot-Tampering in the 21st Century* at 53. https://blackboxvoting.org/black-box-voting-book/ (Last accessed February 10, 2024).
[52] Halderman Report, *Curling v. Raffensberger*, 1:17-cv-2989 (Atlanta Dist. Ct.) at 17.
[53] Tore Maras Declaration, *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020) at 10.
[54] Tore Maras Declaration, *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020), at 17.
[55] Tore Maras Declaration, *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020), at 17.
[56] Tore Maras Declaration, *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020), at 20.
[57] Tore Maras Declaration, *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020), at 16.
[58] Halderman Transcript, *Curling v. Raffensberger*, 1:17-cv-2989 (Atlanta Dist. Ct.) at 141-144.

[59] Complaint, *Philip B. Stark v. United States Election Assistance Commission,* Case No. 1:21-cv-01864 (D.C. Dist Ct. 2021)
[60] Complaint, *Philip B. Stark v. United States Election Assistance Commission,* Case No. 1:21-cv-01864 (D.C. Dist Ct. 2021 at 4.
[61] Complaint, *Philip B. Stark v. United States Election Assistance Commission,* Case No. 1:21-cv-01864 (D.C. Dist Ct. 2021 at 9-10.
[62] Complaint, *Philip B. Stark v. United States Election Assistance Commission,* Case No. 1:21-cv-01864 (D.C. Dist Ct. 2021 at 11.
[63] Complaint, *Philip B. Stark v. United States Election Assistance Commission,* Case No. 1:21-cv-01864 (D.C. Dist Ct. 2021 at 12.
[64] Complaint, *Philip B. Stark v. United States Election Assistance Commission,* Case No. 1:21-cv-01864 (D.C. Dist Ct. 2021 at 12.
[65] https://www.thegatewaypundit.com/2021/01/can-government-agency-certifying-elections-eac-maintain-independence-cio-previously-worked-10-years-dominion-voting-systems/ (Last accessed February 10, 2024).
[66] https://www.thegatewaypundit.com/2021/01/can-government-agency-certifying-elections-eac-maintain-independence-cio-previously-worked-10-years-dominion-voting-systems/ (Last accessed February 10, 2024).
[67] https://www.thegatewaypundit.com/2021/01/exclusive-election-assistance-commission-told-senate-december-2020-two-accredited-test-laboratories-reality-none/ (Last accessed February 10, 2024).
[68] https://www.thegatewaypundit.com/2021/01/exclusive-election-assistance-commission-told-senate-december-2020-two-accredited-test-laboratories-reality-none/(Last acessed February 10, 2024).
[69] FOIA response to request for documentation relating to accreditation of PRO V&V and SCI, December 13, 2023. NIST is the entity which evaluates labs for accreditation under 52 U.S.C. § 20971. NIST criteria for the accreditation process are contained in NIST Handbook 150-22 (2008), "Voting System Testing," available at https://www.nist.gov/publications/nist-handbook-150-22-2008-edition-national-voluntary-laboratory-accreditation-program (Last accessed February 10, 2024). Section 5 of this manual has specific requirements on testing for accreditation, including equipment and calibration requirements.
[70] EAC letter on VSTL accreditation for Pro V&V.
[71] 52 U.S.C. § 20971; VSTL Manual, version 2.0, May 2015, requiring NIST evaluations and recommendations to the EAC for accreditation. According to the VSTL Manual, accreditations are issued for two-year periods and must be renewed by submitting an application package or the accreditation lapses (see VSTL Manual 2.0 at 39), although VSTL Manual 3.0 now appears to have transitioned to a "compliance management program" with biannual "reviews" to avoid lapses in accreditation, starting at 29). https://www.eac.gov/voting-equipment/manuals-and-forms (Last accessed February 10, 2024). Test labs must be compliant with ISO/IEC 17025, *General Requirements for the Competence of Testing and Calibration Laboratories* (VSTL Manual 2.0 at 23 and 3.0 at 24). NIST criteria for the accreditation process are contained in NIST Handbook 150-22 (2008), "Voting System Testing." Section 5 of this manual has specific requirements on testing for accreditation, including equipment and calibration requirements.
[72] https://www.eac.gov/election-officials/voluntary-voting-system-guidelines-vvsg-migration (Last visited February 10, 2024).
[73] https://www.eac.gov/election-officials/voluntary-voting-system-guidelines-vvsg-migration (Last visited February 10, 2024).
[74] VSTL Manual, version 2.0 and 3.0, https://www.eac.gov/voting-equipment/manuals-and-forms (Last accessed February 10, 2024).; Maras declaration, *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020) at 10.
[75] Tore Maras declaration, *Feehan v. Wisconsin Elections Commission* (Case No. 2:20-cv-01771 (E.D. Wis.) (2020), at 16.
[76] Halderman Testimony, *Curling v. Raffensberger*, 1:17-cv-2989 (Atlanta Dist. Ct.) at 242.