IN THE SUPREME COURT OF PENNSYLVANIA

NO. 83 MAP 2013

MARK BANFIELD, *et al.*,

Appellants,

v.

CAROL AICHELE, Secretary of the Commonwealth,

Appellee.

Appeal from the October 15, 2013 Order of the
Commonwealth Court in 442 MD 2006

BRIEF OF APPELLANTS

Michael P. Daly (No. 86103)
Meredith N. Reinhardt (No. 93504)
Katie L. Bailey (No. 308748)
David A. Solomon (No. 312401)
Garrett D. Trego (No. 314496)
Drinker Biddle & Reath LLP
One Logan Square, Suite 2000
Philadelphia, PA 19103-6996

Michael Churchill (No. 4661)
Benjamin D. Geffen (No. 310134)
Public Interest Law Center
of Philadelphia
United Way Building, 2nd Floor
1709 Benjamin Franklin Parkway
Philadelphia, PA 19103

Marian K. Schneider (No. 50337)
Law Office of Marian K. Schneider
295 E. Swedesford Road #348
Wayne, PA 19087

Attorneys for Appellants

Date: January 6, 2014

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page(s)

CASES

CONSTITUTIONAL PROVISIONS

STATUTES, RULES & REGULATIONS

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

I. STATEMENT OF JURISDICTION

Petitioners commenced this action in the Commonwealth Court pursuant to its original jurisdiction. 42 Pa.C.S. §§ 761, 764. It entered judgment on October 15, 2013. This Court has jurisdiction over this appeal from that Order. *Id.* § 723.

II. STATEMENT OF ORDERS IN QUESTION

The Commonwealth Court's Order of October 15, 2013 reads:

> Now, October 15, 2013, judgment in favor of respondent and against petitioners is hereby entered on Counts I, II, III, IV, V, VI, VII, VIII, IX, and X of the petition for review ....

Notice of Judgment (Ex. E).

III. STATEMENT OF STANDARD AND SCOPE OF REVIEW

This Court may reverse an order granting or denying a motion for summary judgment if the lower court committed an error of law or an abuse of discretion. *See Chanceford Aviation Props., LLP v. Chanceford Twp. Bd. of Supervisors*, 592 Pa. 100, 107, 923 A.2d 1099, 1103 (2007). In reviewing conclusions of law or applications of law to fact, the scope of review is plenary and the standard of review is *de novo*. Whether genuine issues of material fact exist is a conclusion of law. *Id.* In making or reviewing such a conclusion, courts view the record in the light most favorable to and any resolve doubts in favor of the nonmovant. *Id.*

IV. STATEMENT OF QUESTIONS PRESENTED

1. Does an electronic voting system ("EVS") allow for a "statistical recount" as required by Section 1117-A if it cannot verify that votes were accurately captured?

Answer to be reviewed: Yes.

2. Does an EVS "provide for a permanent physical record of each vote cast" as required by Section 1101-A if it only stores electronic data as votes are cast and only prints that electronic data (if ever) after an election has ended?

Answer to be reviewed: Yes.

3. Does an EVS "preclude every person from tampering with the tabulating element" as required by Section 1107-A if it has known security vulnerabilities that make it possible to alter votes?

Answer to be reviewed: Yes.

4. Does an examination allow the Secretary to ensure that an EVS "meets all of the requirements" of the Election Code as required by Section 1105-A if it does not test for known security vulnerabilities that make it possible to alter votes?

Answer to be reviewed: Yes.

5. Is the certification of an EVS narrowly tailored to achieve a compelling state interest if, unlike other available EVSs, the EVS cannot verify that votes were accurately captured?

Answer to be reviewed: Yes.

V. STATEMENT OF THE CASE

A. Form of the Action and Procedural History

Petitioners filed this action on August 15, 2006. (R. 109a). On August 29, 2012, the Commonwealth Court denied Petitioners' Motion for Partial Summary Judgment on Counts I, IV, V, and VI. (Ex. A., 51 A.3d 300) On January 29, 2013, it dismissed those counts. (Ex. B). On October 1, 2013, in an unreported Memorandum Opinion, the Commonwealth Court granted the Secretary's Motion for Summary Judgment on Counts II, III, VII, VIII, IX and X. (Exs. C & D). On October 15, 2013, it entered a final judgment against Petitioners on all counts. (Ex. E). This appeal followed.

B. Statement of Determinations Below

The relevant determinations below are attached as Exhibits A through E. The Honorable Bonnie Brigance Leadbetter authored the opinions. The Honorable Patricia McCullough and Dan Pelligrini dissented from the August 2012 opinion.

C. Statement of Facts

1. The Election Code and Voting Machines

The Election Code was codified in 1937.[1] For 43 years, it only allowed voting with ballots[2] or lever machines.[3] Whereas ballots could be "recounted" if

---

1 Act 1937-320, P.L. 1333, 25 P.S. §§ 2600-3591 (1937).

2 Article X, 25 P.S. §§ 2961-71.

3 Article XI, 25 P.S. §§ 3001-18.

an election were contested,[4] lever machines created no records of individual votes and thus could only be "recanvassed."[5]

An amendment proposed in 1971 would have allowed voting with EVSs.[6] As the Secretary's expert put it, the General Assembly "recognized a deficiency in lever machines, which did not produce individual vote records" and "when the polls close ... show only cumulative totals." (R. 719a, 763a-64a). The EVSs that existed at that time (optical scan and punch card systems) did not have those deficiencies because they used individual vote records that could be recounted.

Even so, the amendment was opposed by legislators who had concerns about "the possibilities of fraud" that could be "impossible to detect" without additional "safeguards."[7] It was not until 1980—by which time the amendment had been revised so that it had "as much security check as possible"[8]—that the code was finally amended.[9] As amended, it allows EVSs only if they:

- allow a "statistical recount" after each election[10];
- "provide for a permanent physical record of each vote cast"[11];

---

4 Article XVII, 25 P.S. § 3261; Article XIV, 25 P.S. § 3154(e)(2).

5 Article XVII, 25 P.S. § 3262; Article XIV, 25 P.S. § 3154(e)(1).

6 H.B. 1366, 1971-72 Gen. Assemb., Reg. Sess. (Pa. 1971).

7 (R. 1505a-06a (Statement of Rep. Taddonio, July 2, 1980); (R. 2910a-13a (same, June 26, 1974)). We discuss the legislative history at length *infra* Section VII.A.1.

8 (R. 2913a (Statement of Rep. Taddonio, June 26, 1974)).

9 Act Amending the Pennsylvania Election Code, P.L. 600, No. 128 (Pa. 1980).

10 Section 1117-A, 25 P.S. § 3031.17.

- "preclude every person from tampering with the tabulating element"[12];
- "provide[] acceptable ballot security procedures ... to prevent tampering with or substitution of any ballots"[13]; and
- are tested for compliance with "all of the requirements" of the code.[14]

Years after the code was amended to allow EVSs, direct-recording electronic ("DRE") systems were developed.[15] Unlike optical scan and punch card systems that use physical ballots with physical data (marks or holes) that are created by voters and read by electronic devices, DREs use digital ballots with electronic data that is created by software, is readable only by software, and is not printed (if ever) until after polls close.[16] The systems challenged here (the Danaher ELECTronic 1242, ES&S iVotronic, Hart eSlate, Diebold AccuVote TSx, and Sequoia Edge 2 and Advantage) are DREs.

---

11 Section 1101-A, 25 P.S. § 3031.1.

12 Section 1107-A, 25 P.S. § 3031.07(16)(iii), (17)(i).

13 *Id.* § 3031.7(12).

14 Section 1105-A, 25 P.S. § 3031.5(b).

15 DREs were used by one county in 1983 and were not widely available until 1987, when the Shouptronic ELECTronic was patented. (R. 763a-64a, 895a-98a, 1492a).

16 Data about individual votes is called a "ballot image retention" or "BIR." BIRs are not printed unless an official does so after polls close, at which point the data has existed exclusively in electronic form for hours. (R. 894a, 763a). As the lower court found, BIR is a "misnomer" because "neither a ballot image nor a reproduction of the visual screen image is actually provided. (Ex. A at 8 n.18). Although DREs can be retrofitted with a voter verified paper audit trail ("VVPAT") device that prints records as votes are cast and non-sequentially drops them into a receptacle after it is reviewed, none of the challenged DREs has such a device. (R. 1494a).

2. The Rush to Certify the Challenged DREs

The Help America Vote Act (HAVA), 42 U.S.C. § 15301 *et seq.*, allocated funds for replacing lever machines and punch card systems. To receive them, states had to comply with HAVA by the first federal election after January 1, 2006. Although optical scan machines were available, several manufacturers sought to certify DREs and it was "all hands on deck" as the federal deadline approached.[17]

It was in that environment that the challenged DREs were first examined. The examiners reviewed no source code and conducted no penetration analyses.[18] Instead, they relied on independent testing authorities ("ITAs") to do that.[19] This despite the fact that one of the Secretary's examiners (Michael Shamos, also her expert in this proceeding) believed ITA testing was "dysfunctional" and "virtually nonexistent."[20] The result was the equivalent of kicking the tires to test the car—

---

[17] (R. 864a (Dep. at 22:13-14); R. 985a ("Everyday that goes by without additional certified systems puts the Commonwealth, particularly the Department, in a terribly [sic] predicament.")).

[18] (R. 2983a, 2986a, 2991a (Dep. at 76, 86, 106); R. 3094a-96a, 3101a (Dep. at 166-67, 170-71, 186-87, 253)). "Source code[s]" are instructions that are compiled into an executable computer program. A "penetration analysis" is a test for identifying security vulnerabilities.

[19] ITAs were created by the National Association of State Election Directors to standardize voting system testing among states. (R 745a). Congress incorporated the system into voting system certification in HAVA, 42 U.S.C. § 15371. Vendors hired and paid the ITAs, creating incentives for ITAs to approve the vendors' systems. (R. 839a-40a).

[20] (*See* R. 859a ("Some of these systems contain security holes so glaring that one wonders what the ITA was looking for .... Many states that formerly had statutory certification procedures have abdicated them in favor of requiring no more from a vendor than an ITA qualification letter .... We are less safe in 2004 than we were 20 years ago."); R. 2971a-72a, 2976a) (Dep. at 27, 30-31, 47)).

examinations of few things by a few people for a few hours and reliance on ITAs the examiners knew were unreliable.

3. Computer Experts Identify Flaws in DRE Security and Reliability

a. The 2005 Brennan Center Report

In 2005, the Brennan Center for Justice (a non-partisan public policy group) convened a task force of "voting machine experts and security professionals" to analyze vulnerabilities in voting systems, including the Sequoia AVC Edge, Sequoia AVC Advantage, ES&S iVotronic and Diebold Accuvote-TSx. (R. 3106a). It found that they lacked "a powerful countermeasure to software attacks," which is problematic because they lack "voter-verified paper trails...." (R. 3118a). It concluded that "attacks that involve the insertion of ... corrupt software are the least difficult" in statewide elections and saw "no reason why the methods used ... cannot be applied to local (or national) races." (R. 3116a-17a).

b. The 2006 Princeton Report

In 2006, Princeton University researchers analyzed the AccuVote TS, the predecessor of the AccuVote TSx. They concluded that "the machine is vulnerable to a number of extremely serious attacks that undermine the accuracy and credibility of the vote counts it produces." (R. 3265a). They also identified attacks that could be performed in real elections, for example how malicious code could be installed in less than one minute and then spread from one machine to another. (R. 3268a-70a). They concluded that:

> DREs are much more vulnerable to large scale fraud. Attacks on DREs can spread virally, they can be injected far in advance and lurk passively until election day, and they can alter logs to cover their tracks. Procedures designed to control small-scale fraud are no longer sufficient—DREs demand new safeguards. (R. 3285a).

c. The 2007 Florida Report

In 2007, Florida's Secretary of State issued a report based on independent testing by the SAIT laboratory.[21] The report concerned a newer version of the AccuVote TSx and the same version of the GEMS software used in Pennsylvania. It highlighted a scenario in which an attacker could prepare:

> official, activated voter smart cards that would enable voters to cast multiple ballots in a ballot-stuffing attack. Creation of the cards requires an adversary able to insert a custom smart card into a legitimate voting terminal and to read the data off of a valid voter card .... Once the adversary obtained the necessary information in this way, she could then create smart cards that could be used at any precinct throughout a county. Even if detected, this attack is not correctable: the malicious ballots, either in electronic or paper form, are essentially unidentifiable ....[22]

d. The 2007 California Top to Bottom Review

In 2007, California conducted a "Top to Bottom Review" in which source code reviews and penetration analyses revealed vulnerabilities in the AccuVote

---

21 *See* Ryan Gardner et al., *Software Review and Security Analysis of the Diebold Voting Machine Software*, Fla. Stat. Univ. (2007) *available at* www.cs.jhu.edu/~rubin/SAIT.pdf ("FL SAIT Report"); (*see also* R. 3449a-82a (Supplemental Florida SAIT Report)).

22 FL SAIT Report at 3-4.

TSx, eSlate and AVC Edge 2. (R. 3483a-542a). Petitioners' expert explained that the California review showed that a voter can use "a few easily concealed tools, can reset the TSx DRE to administrative mode, delete all ballots cast thus far on the machine, and restart the election on the unit"; that the eSlate's software "often fails to check the validity of input values it receives from outside sources, opening the system to a common type of attack that is frequently used by 'hackers' to take control of computers over the Internet"; and that the AVC Edge 2's firmware "provides commands for setting the supposedly tamper-proof protective counter of the machine ... overwriting other software and firmware in the system (including the audit trail), and rebooting the machine at will." (R. 1007a). California decertified them, later conditionally recertifying some for use by persons with disabilities if enhanced security measures and audit procedures were observed.

e. The 2007 Ohio EVEREST Report

Ohio's EVEREST study caused the Ohio Secretary of State to recommend decertifying DREs. (R. 1377a-462a). Petitioners' expert explained that the Ohio report found that the AccuVote TSx had a "common type of programming error" that "can be exploited by an attacker to run arbitrary code on the DRE which can then propagate to other components"; that the eSlate "generates supposedly 'random' voter access codes that are easy to predict," which would "allow an

attacker to vote multiple times using the DRE"; and that the iVotronic "can be rebooted by a voter with the use of a simple magnet." (R. 3638-3639a).

f. The 2011 Argonne National Laboratory Test

In 2011, the director of the Vulnerability Assessment Team at the Argonne National Laboratory (a research laboratory operated by the University of Chicago) demonstrated how to perform a "man in the middle" attack on an AccuVote TSx and an AVC Advantage with less than $30 of equipment and less than one minute inside the voting booth. The attack allowed him to manipulate subsequent votes in a manner that would be invisible to voters and undetectable to officials: "It's a classic attack on security devices. You implant a microprocessor or some other electronic device into the voting machine, and that lets you control the voting and turn cheating on and off...." (R. 3600a). He stated that "[a]nyone who does digital electronics—a hobbyist or an electronics fan—could figure this out." *Id.*

g. The Testimony of Petitioners' Experts

Petitioners' experts, Dr. Jones and Dr. Lopresti,[23] testified that the challenged DREs have vulnerabilities that make it possible to tamper with their ballots (R. 3610a, 3637a) and tabulating elements (R. 3607a-08a) in live elections without detection (R. 3609). They also opined that pre-election testing and other

---

[23] Dr. Jones is an Associate Professor in the Department of Computer Science at the University of Iowa. (R. 891a-92a). Dr. Lopresti chairs the Department of Computer Science and Engineering at Lehigh University. (R. 1001a-02a). Neither receives compensation for their services as witnesses in this proceeding. (R. 892a, 1010a).

purported safeguards are not effective at preventing or detecting fraud. (R. 903a, 1009a, 3611a).

4. The Secretary Recertifies the Challenged DREs

Petitioners requested reexaminations in 2006. Although one of her initial examiners (Dr. Shamos) thought that the California and Ohio reports identified "important security issues" that "should be considered by the Secretary" in deciding what "might be undertaken to counteract their security vulnerabilities,"[24] the Secretary waited five years before reexamining them and retained an examiner who had only a vague understanding of only a few of the reports noted above.[25] His security testing consisted of little more than checking that locks, seals and passwords existed, but not checking whether he could pick the locks, could bypass or break the seals, or learn the passwords from reviewing the source code.[26] When asked why, he said that doing more would have been beyond the scope of his engagement.[27]

---

24 (R. 756a, 767a; *see also* R. 3706a ("Some of these vulnerabilities are severe and require immediate repair.")).

25 (*See* R. 3876a-77a, 3894a (Dep. at 131-132, 137, 205)).

26 (*See* R. 3874a, 3882a, 3885a-86a, 3890a (Dep. at 154, 169-70, 188)).

27 (R. 3878a-79a (Dep. at 141-42)).

VI. SUMMARY OF THE ARGUMENT

Voting is a fundamental right that the state cannot unnecessarily burden. The legislature tried to protect this fundamental right by including a number of safeguards in Article XI-A, including two that minimize the risk that the votes reported by the machine are different from the votes cast by the voters. That risk arises because there is no way to know if what comes out of the machine is accurate if that is all you look at. The legislature therefore required that EVSs "provide for a permanent physical record of each vote cast" and be subjected to a "statistical recount" by a device (method) different from that used in the election. The requirements are inter-related, as there would be no way to recount the votes by a different device if there were no permanent physical record of each vote cast.

The Secretary has interfered with the fundamental right to vote by certifying DREs that do not meet these requirements even though other kinds of EVSs do. The lower court upheld that decision. To do so, it found that a print-out of data that existed exclusively in electronic form throughout the course of the election is a "permanent physical record of each vote cast" and that a re-tally of computer-generated data (such as the print-outs) is a "recount" by a different device. This construction is contrary to the actual language of the statute; to the legislative history, which evinces a focus on assuring that EVSs had not been tampered with;

and to the constitutional requirement that nothing interfere with voters' ability to have their vote counted.

The need to construe these requirements rigorously is particularly important in light of Petitioners' evidence that the risk of undetectable tampering is real. Granting summary judgment against Petitioners on the grounds that tampering is only a "possibility" misreads the statute, misunderstands the legislative history, and misapprehends the need to protect the fundamental right to vote from attacks that could happen, not merely attacks that have happened. The Secretary did not exercise her discretion in accordance with the law in certifying that the challenged DREs comply with the Election Code because she did not even investigate a number of well-documented vulnerabilities.

The lower court ignored the constitutional protection of the right to vote, treating the Secretary's actions as subject to a high level of deference that is inappropriate when reviewing constitutional rights. It never addressed directly the constitutional claims nor whether there was any compelling reason for tolerating well-documented risks to the right to vote when there are alternative EVSs that protect that right by creating recountable records of each vote the moment it is cast.

VII. ARGUMENT

A. DREs Do Not Allow A "Statistical Recount" As Required By Section 1117-A (Count IV)

EVSs are unique in that, no matter how close the election, their results must be subjected to a "statistical recount of a random sample of ballots after each election using manual, mechanical or electronic devices of a type different than those used for the specific election." Section 1117-A, 25 P.S. § 3031.17. The lower court held that DREs satisfy Section 1117-A because the statute was not meant "to verify whether the EVS correctly captured voter intent," "does not require software-independent vote records," and is satisfied so long as "printed copies of the electronically recorded vote records ... can be counted manually." Ex. A at 19-22. That was an error of law.

1. Section 1117-A Was Meant To Verify Voter Intent

We begin with Section 1117-A's plain language. *Dechert LLP v. Commonwealth*, 606 Pa. 334, 340, 998 A.2d 575, 579 (2010). Although the words are not defined, it has long been understood that a "recanvass" only checks whether votes were correctly ***counted***, whereas a "recount" also checks whether votes were correctly ***captured*** in the first place. *Edwards v. Prutzman*, 108 Pa. Super. 184, 186-87, 165 A. 255, 255 (1933) ("The recounting of the votes ... is to ascertain whether there is any fraud or substantial error appearing. This requires something more than the mere counting of the votes. It involves the exercise of

judicial functions to decide whether certain votes shall be counted or not.").[28] The archetypal example is the Florida recount of 2000, which would not have been possible without ballots and hanging chads. *Cf. In re Gen. Election for Twp. Supervisor*, 152 Pa. Cmwlth. 590, 596, 620 A.2d 565, 568-69 (1993) ("A recount is the opening of a ballot box and the recount of the votes.... A recanvass is the opening of a voting machine in order to check the counters inside the machine which record the number of votes...."); Pa. Law Encyclopedia § 105 (2d ed. 2011) ("Ballots may be recounted and voting machines may be recanvassed.").

That meaning is also evident from the rest of the Election Code, which uses the words distinctively. 25 P.S. § 2121 (ordering "recount or recanvass of an election"); *id.* § 2650 (observing "recount of ballots or recanvass of voting machines"); *id.* § 3154(b) (discussing "recount of the ballots contained in said ballot box"); *id.* § 3154(d)(1) (same); *id.* § 3157 (appealing from "recount or recanvass"); *id.* § 3261(a)(1) (allowing recounts and requiring court to "open the ballot box of each election district in which ballots were used" and "cause the entire vote of the election district to be correctly counted"); *id.* § 3262 ("recanvass"

---

[28] *See also* Clifford B. Levine & David J. Montgomery, *Post-Election Litigation in Pennsylvania*, 41 Duq. L. Rev. 153, 160 (2002) ("Unlike the recount of punch card ballots ... a recanvass of the machine is aimed strictly at mechanical or mathematical error."); Candice Hoke, *in America Votes! A Guide to Modern Election Law & Voting* 324 (Benjamin E. Griffith, ed., 2012) ("systems [that] require voters to mark a paper ballot that is then read by an optical scanner ... permit the extrinsic paper record to be used ... in post-election audits or recounts."); *see also id.* at 387 n.99.

provision requiring court to "make visible the registering counters of the voting machine" and "without unlocking the machine against voting, ... recanvass the vote cast therein"); *id.* § 3263 (petitioning to "open a ballot box or to recanvass the votes"); *id.* § 3506 (barring observers from "recount of ballots or recanvass of voting machines" penalized). The General Assembly used different words because it attached different meanings to them. *Fonner v. Shandon, Inc.*, 555 Pa. 370, 378, 724 A.2d 903, 907 (1999).

And if there were any doubt about the plain meaning of the word "recount," there can be no doubt about what the General Assembly meant. Article XI-A was the result of nearly ten years of debate. It was opposed by legislators who believed EVSs were unsound and unsafe, and who refused to support it until it was revised to require a statistical recount that would deter and detect fraud. (R. 2910a-13a (Statement of Rep. Taddonio) ("The proponents of the measure maintain that no evidence of fraud has ever been found in voting systems of this type .... The reason for not having exposed any fraud could be ... that the fraud is there but it has not been discovered. In other words, it could be impossible to detect .... I submit that the only thing we know for sure is that there are serious questions as to the accuracy and security of this system."); R. 2913a (*id.*) ("I was interested in getting amendments that would strengthen the bill .... I was interested, if it did pass, to have as strong a bill as possible with as much security check as possible.");

R. 2918a-19a (*id.*) ("This change [EVSs], in my opinion, would open up the door and the floodgates to a lot of potential fraud. ... I imagine Mr. Sweet is later going to come out and say that there have been no cases of election fraud brought out in places which use the computer voting system. That may be true, but it does not mean they do not exist. ... I think that Mr. Sweet is also going to bring out the possibility that there are many safeguards in the bill. I know there are; I put them in there in 1974. ... One of them is for a statistical recount. It provides that 2 percent of the votes shall be recounted by some other means. That is a safeguard.")).[29]

Notably, when the General Assembly singled out EVSs for automatic "recounts," every EVS in existence was a punch card or optical scan system that created a recountable record of every vote as it was cast.[30] In other words, every "recount" that had ever been conducted in the Commonwealth had involved ballots from which voter intent could be determined. Nothing in the legislative history suggests that the General Assembly had something else in mind. On the contrary, the Secretary's own documents confirm that the Election Code "contains a very heavy bias toward systems using punch cards (now replaced) or optical scan

---

[29] The lower court's citation to the legislative history actually suggests that Representative Taddonio was blasé about the risks of EVSs. Ex. A at 17 n.29. For their part, the Secretary and her expert took the equally incredible position that "[t]he 'authors' of the statute were the voting system vendors themselves." (R. 729a).

[30] *See supra* note 15.

electronic voting systems. Because DRE's [sic] arrived on the market after the enactment of Act 128, it is often ambiguous in the application of its provisions to the requirements of DRE systems." (R. 1492a).

In light of its "unambiguous words," the "mischief to be remedied," the "circumstances under which it was enacted" and the "contemporaneous legislative history," 1 Pa.C.S. § 1921(c), Section 1117-A was meant to verify voter intent. Ex. A at 20. The lower court erred in finding otherwise.

2. "Print[ing] copies of the electronically recorded vote records ... that ... can be counted manually" Does Not Satisfy Section 1117-A

The meaning of the word "recount" is determinative because the parties agree that there is no way to check whether the challenged DREs correctly capture voter intent. One cannot test the accuracy of what comes out of a machine without knowing what went into it. As the Secretary conceded below, DREs do not allow us to test "whether a voter's intent was properly recorded by the machine." (R. 435a). And as her expert has testified, if a "voter's intentions were frustrated" before a vote was recorded, "there's just simply no way of proving that there's ever been any tampering. You ... can count and recount and count the votes 50 times and you'll get the same totals. They'll just be wrong ...." (R. 3323a-25a; *see also* R. 751a ("[A] system is accurate if it captures voter intent correctly.... This form of accuracy is very difficult to measure because there must be some independent

way of learning the voter's intent aside from the voter's interaction with the system. Only then can intent be compared with what was actually captured.")).[31]

And even if we assume for argument's sake that DREs can be "recounted," they cannot be recounted by using "devices of a type different than those used in the specific election." 25 P.S. § 3031.17. DREs save election data to electronic memory. (R. 1003a-04a). Because there is no data separate and apart from that electronic memory, it would be impossible to generate election data with a device other than the one that created it. (R. 898a-99a, R. 1005a-06a).

The lower court found that printing computer-generated data and comparing it with computer-generated election results is acceptable because "Section 1117-A provides only that the statistical sample of ballots must be *counted* using a different method or device; there is no requirement that the ballots included in the recount must be produced using a separate device." Ex. A at 20 (emphasis in original). That contradicts the plain language of the statute, which says recounts must be "conducted" using different devices. Moreover it defeats the purpose of a recount.

---

[31] *See also* Hoke, *supra* note 28, at 357 ("Recounting using an extrinsic record independent of the software should be recognized as essential for preserving voting rights and become a routine practice when computer-based voting equipment is deployed."); *id.* at 379 n.56 ("a paper record ... created contemporaneously with the voter's ballot casting ... can then be used as a check on the invisible electronic record via recounts"); United States Association of Computer Machinery, E-voting, *available at* http://usacm.acm.org/evoting ("Voting systems should also enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and stored by the system. Making those records permanent (i.e., not based solely in computer memory) provides a means by which an accurate recount may be conducted.").

The "recount" the lower court blessed here is the intellectual equivalent of comparing photocopies; the process could tell whether the copies are the same, but could never tell whether either of them transmits an accurate copy of the original. The only way to do that is to have the original—something DREs never produce. Contrast what the lower court approved for DREs with what can be done with the optical scan and punch card systems that were in existence when the Election Code was amended in 1980. In short, to find that DREs can be "recounted," the lower court had to change the very meaning of the word.

3. By Requiring that EVSs Be Recounted, the Election Code Does Require That EVSs Create "Software-Independent Vote Records"

Ignoring Section 1117-A's language and legislative history, the lower court cited Section 1404(e) for the proposition that the Election Code "does not require software-independent vote records." Ex. A at 20. But that ignores that the relevant language in Section 1404(e) was added in 2004—***24 years after Section 1117-A***.[32]

---

[32] The lower court also cited Section 1101-A's definition of "voting device" for the proposition that the Election Code "authorizes systems which only register votes electronically." Ex. A at 20. But that does not mean EVSs are relieved from satisfying the "permanent physical record" requirement. On the contrary, EVSs may use "one or more voting devices," Section 1101-A, 25 P.S. § 3031.1, meaning they can "register" votes electronically so long as they also create recountable "records." An example would be Lackawanna County's ES&S AutoMark, which uses an electronic "device" to mark ballots, another electronic "device" to count them, and creates a recountable "record" of each vote in the process.

In 2004, the Election Code was amended to facilitate statewide review in the event of a close election like Florida's 2000 election.[33] The amendments require that "an electronic voting system utilizing paper ballots" be subjected to a "recount" using "manual, mechanical or electronic devices of a different type used for the specific election,"[34] and "any other type of electronic voting system" be subjected to a "recanvass."[35] In other words, they acknowledge what Petitioners have been arguing all along—that DREs cannot be "recounted" at all.

The lower court saw the 2004 amendment not as an acknowledgement that DREs were unable to be "recounted," but as an acknowledgement that DREs were "authorize[ed]." Ex. A at 20. It held essentially that the amendments implicitly repealed the "statistical recount" provision that had been a part of the Election Code for 24 years. *Id.*

That was an error of law. "Repeals by implication are not favored and will not be implied unless there be an irreconcilable conflict between statutes embracing the same subject matter.... [T]he legislative intent to repeal a statute by enacting another must be clearly shown. The reason for such a restriction is obvious: absent irreconcilability, a judicial finding of implied repeal would

---

33 See Legislative Journal – House, at 1732-33 (No. 58, Oct. 6, 2004) (Statement of Rep. Smith) ("The perceived purpose ... is to ensure that if we are engaged in a close election in Pennsylvania, that the ballots will be recounted in an expeditious manner....").

34 Section 1118-A, 25 P.S. § 3031.18(1); Section 1404(e), 25 P.S. § 3154(e)(3).

35 Section 1118-A, 25 P.S. § 3031.18(2); Section 1404(e), 25 P.S. § 3154(e)(4).

essentially rewrite the legislation." *HSP Gaming LP v. City of Philadelphia*, 598 Pa. 118, 151, 954 A.2d 1156, 1175 (2008) (citing 1 Pa.C.S. § 1971) (citations omitted). Here, there is no irreconcilable conflict and nothing in the legislative history shows that the General Assembly meant to repeal or revise Section 1117-A.

First, there is no irreconcilable conflict because Section 1404(e) does not "authorize[] the use of" DREs. Ex. A at 17. There would be an irreconcilable conflict if Section 1404(e) prohibited EVSs from producing recountable records, but that is not what it says. Section 1404(e) simply creates a process for auditing a kind of EVS if it happens to be used. A separate provision that has the effect of prohibiting that kind of EVS from being used may mean the former is dormant, but it does not create "surplusage," let alone an "irreconcilable conflict."

Second, there is no indication that the General Assembly meant to repeal Section 1117-A. On the contrary, the legislative history reflects that there was little time to debate anything other than the lack of time for debate.[36] What's more, the chief proponent of Section 1404(e) stated that its purpose was to increase voter confidence by ensuring that elections reflect "the intent of the voters."[37] How can

---

[36] *See* Legislative Journal – House, at 1726 (No. 58, Oct. 6, 2004) (Statement of Rep. Casorio) ("this is ... 21 pages of Election Code language ... that was thrust upon us, Madam Speaker, a mere 30 minutes ago. Madam Speaker, we are rushing to judgment here."); *id.* at 1729 (Statement of Rep. Manderino) ("in our rush to do things, we always have to stick in a few extra goodies that may have complications that we have not yet perceived....").

[37] *See id.* at 1732-33 (Statement of Rep. Smith) ("The perceived purpose ... is to ensure that ... ballots will ... reflect the intent of the voters.... [I]t will give the voters of Pennsylvania the fullest amount of confidence that we can bestow upon them that their ballot, that their vote, will

we read the amendments as implicitly repealing the protection of Section 1117-A when the legislature meant to ensure it?

The lower court resolved the tension between Sections 1404(e) and 1117-A by finding that the former (which creates a procedure for recanvassing DREs) is surplusage if the latter (which requires a recount for all EVSs, including DREs) prohibits DREs. Ex. A at 21-22. But to do so it had to "rewrite the legislation" by reading "recount" in a way the General Assembly did not intend. *HSP Gaming*, 598 Pa. at 151, 954 A.2d at 1175. That was error. In a case that concerns preventing fraud and protecting votes, an interpretation that renders a procedural protection redundant should be preferred over an interpretation that destroys one. *Shambach v. Bickhart*, 577 Pa. 384, 392, 845 A.2d 793, 798 (2004) ("election laws must be strictly construed to prevent fraud" and "construed liberally in favor of the right to vote"). Similarly, an interpretation that renders a statute constitutional should be preferred over one that renders it unconstitutional. *In re William L.*, 477 Pa. 322, 329, 383 A.2d 1228, 1231 (Pa. 1978). And as noted below, the unnecessary elimination of an important safeguard of the fundamental right to vote

---

in fact count and will be reflected accurately in the final count.... [O]ur right to vote is singularly the most important in that regard, and the only thing that gives it true power is the fact that the voters would know that their vote was counted and counted accurately."); *id.* at 1735 ("[T]his amendment ... will ... empower[] the voters to know that in fact their vote was counted; win or lose, they know that it was counted accurately....").

would not have survived strict scrutiny had the lower court addressed that claim. *See infra* Section E.3.

The lower court's error becomes clear when one applies its reading of "statistical recount" to EVSs other than DREs. Take for example an optical scan system that incorrectly records 10% of the votes for candidate "A" as votes for candidate "B." Under Petitioners' reading of Section 1117-A, a county would have to examine a statistical sample of actual ballots, which could detect that error. But under the lower court's reading of Section 1117-A, the county could simply check the system's tabulation, which could not detect that error. That was not what the General Assembly intended.[38]

* * * * *

The great irony of DREs is that they turn the lesson of 2000 on its head.[39] That lesson was not that manual recounts are messy or costly. Rather, it was that recounts, no matter how messy or costly, are absolutely necessary. And it is no exaggeration to say that they are absolutely impossible with DREs. The consequence—indeed, the purpose—of a secret ballot is that only one person on Earth—the voter—knows how a vote was cast. When the voter leaves the polling

---

[38] Even the Secretary recognizes this, as she has instructed counties to manually recount paper ballots to comply with Section 1117-A. (R. 1509a-13a).

[39] As the Secretary's office put it, "now the voting systems that were meant to resolve the problems of the 2000 election are viewed by many as the problem." (R. 1496a).

place, it is impossible to match up voter and vote. It follows that the only way to verify that voter intent was captured correctly is to create a permanent physical record of it the instant it is cast. The challenged DREs do not do that. The most they do is regurgitate electronic data days or weeks later, after it has been mediated by the firmware, software, and anyone who had access to either of them.

In short, if the indelible image of the 2000 election was a Florida election worker squinting at a chad, the indelible image of the next election could be a Pennsylvania election worker shrugging at a DRE. Although by no means perfect, optical scan systems give voters confidence that votes can be counted as intended, and can be recounted to verify that they were. The DREs used in Pennsylvania can do neither of those things, and no amount of whistling past the graveyard will ever make it otherwise. It follows that the lower court should have granted Petitioners' Motion for Summary Judgment.

B. DREs Do Not "Provide For A Permanent Physical Record Of Each Vote Cast" As Required By Section 1101-A (Count I)

Section 1101-A requires that every EVS "shall provide for a permanent physical record of each vote cast." Section 1101-A, 25 P.S. § 3031.1. As their name suggests, DREs create electronic data as votes are cast and do not print it (if ever) until after it existed exclusively in electronic form for hours (if not longer). The lower court held that this satisfies Section 1101-A. In doing so, it found that "provide for" means records can be created "on demand" long after a vote is cast,

that data is "permanent" so long as it "serves the purposes of the Election Code," and that DREs "generate a paper record of each vote cast." Ex. A at 7-8, 11-12.

That was error. There are two candidates for the permanent physical record the Election Code requires: the electronic data that are created as votes are cast, and the physical data that can be printed from electronic data after polls close. Because neither satisfies Section 1101-A, the lower court should have granted Petitioners' Motion for Summary Judgment.

1. Although DREs Do "Provide for" Electronic Data, That Data Is Not "Permanent," "Physical," Or A "Record of Each Vote Cast"

Electronic data does not satisfy Section 1101-A for three principal reasons. First, as Judges McCullough and Pelligrini found, it is not "physical." Ex. A, Dissent at 3. Even the majority was unwilling to hold that electronic data is "physical" (Ex. A at 15), and even the Secretary's expert once accepted that paper is physical and electronic data are not. (R. 3356a-57a ("you press the exit button which causes the recording of these votes and they're recorded in three different ways; a permanent physical record is made of your ballot. That is it goes on ... a roll of paper tape so that it can be reconstructed later. It's also recorded electronically....")).

That makes sense, as "the electrons used to record data ... cannot be observed without the aid of complex technology...." (R. 895a); *see also* Webster's Ninth New Collegiate Dictionary at 887 (1984) ("physical. 1a: having material

existence; perceptible esp. through the senses ....")). Although courts have struggled with the nature of electronic data in other contexts, ultimately the answer turns on what the General Assembly intended.[40] Here, it could not have meant for subatomic particles to satisfy Section 1101-A. First, it must have meant for "physical" to mean ***something***. 1 Pa.C.S. § 1922; *Hamilton v. Unionville-Chadds Ford Sch. Dist.*, 552 Pa. 245, 249, 714 A.2d 1012, 1014 (1998). But the lower court's reading of "physical" adds nothing, as by their nature EVSs necessarily store electronic data. Second, it must have meant for "physical" to mean ***something other than electronic***. Otherwise it could have required a "permanent electronic record." It knew how to use the word "electronic" when it wanted to. Indeed, it used the word in the preceding sentence. It used a different word there because it attached a different meaning to it. *Fonner*, 555 Pa. at 378, 724 A.2d at 907. It follows that electronic data are not "physical" for purposes of Section 1101-A.[41]

Second, electronic data are not "permanent." The lower court held that "permanent" requires that a record "serves the purposes of the Election Code,"

---

[40] For example, in deciding whether software is "corporeal" for purposes of being taxable, this Court's analysis turned less on metaphysics than on whether the General Assembly intended for software to be taxed. *Dechert*, 606 Pa. at 347-48, 998 A.2d at 583-84.

[41] The Secretary has argued that Petitioners read Section 1101-A as requiring ***paper*** records. While paper is the most obvious physical medium for recording votes, the Election Code does not rule out other "physical" records, for example punch cards (which were widely used in 1980) or any other physical medium that the market may demand.

meaning it will be "intact and be available for an indefinite period of time, but at a minimum, twenty days for ... state-related contests and twenty-two months in federal-related election matters." Ex. A at 11-12. But nothing in the language or history of Section 1101-A suggests that the General Assembly meant for "permanent" to mean different things in different elections. And not even the Secretary's expert was willing to argue that a mere twenty days is "permanent."[42]

Moreover, the proper focus is not on how long data can be retained, but on whether it can be altered. Black's Law Dictionary at 1139 (6th ed. 1990) ("Continuing or enduring in the same state ... without fundamental or marked change, not subject to fluctuation, or alteration, fixed or intended to be fixed; lasting; abiding; stable; not temporary or transient...."); Webster's Ninth New Collegiate Dictionary at 877 (1986) ("continuing or enduring without fundamental or marked change: STABLE."). By its nature, electronic data can be altered whenever an EVS is in use, meaning the data regarding a vote cast in the morning are in an alterable (and thus impermanent) state until the polls close in the evening. What's more, as Petitioners' experts explained, those alterations are "in principle undetectable" because they "leave behind no physical evidence." (R. 1004a-05a; *see also* R. 893a-94a). Data on a memory card is only arguably "permanent" if the memory card is separated from the computer, at which point it may no longer

---

42 (R. 742a; R. 727a (referring to federal "22-minth [sic] ballot retention requirement."))

reflect the vote that was cast. And it would only be useful as a "record" if it were reconnected to a computer, at which point it would no longer be "permanent." (R. 894a (noting that electronic data are "resistant to human interpretation")).

Finally, electronic data are at best a "record" of what the software created, and it is unknowable if they actually are a record of what the voter intended. Even the initial writing of electronic data is affected by software. As Petitioners' expert explained, because one cannot be certain that software is not flawed or corrupted, one cannot be certain that the data reflects voter intent. (R. 1005a ("Since even the initial writing of a record into computer memory is accomplished through the use of software and hardware intermediaries, there is no way for a human observer to confirm that what is written is in fact an accurate record....")). In short, whereas optical scan systems use voter-created "records," DREs use software-created data that may or may not reflect what actually happened.[43]

2. Although DREs Can Print Data on Paper That Is "Physical" and Arguably "Permanent," They Do Not "Provide For" A "Record of Each Vote Cast"

The lower court focused not on the electronic data that are created while polls are open, but on paper that could be printed from those data after polls close.

---

[43] Notably, the Secretary instructed counties that they may reuse memory cards in each election (R. 1467a), which she could not have done if the memory cards were actually "records" of votes. 42 U.S.C. § 1974 (requiring preservation of "all records ... relating to an ... act requisite to voting").

Although such documents are admittedly "physical" and arguably "permanent,"[44] they do not satisfy Section 1101-A because they are no more a record of each vote cast than the software-dependent electronic data from which they must be printed. The lower court was wrong to say it was "undisputed that the DREs ... can generate a paper record...." Ex. A at 8. While Petitioners do not dispute that DREs can create paper ***documents***, they do dispute that DREs create a paper ***"record of each vote cast."*** Indeed, they proved otherwise.

DREs do not print out a BIR in the normal course of their operation and nothing in the record suggests that counties normally do so.[45] The lower court found that DREs satisfy Section 1101-A anyway. It held that "provide for" does not mean an EVS must ***provide*** a record "automatically with each vote cast," but instead means that it be ***capable of providing*** a record "on demand." Ex. A at 7. But that contradicts the plain meaning of, and unnecessarily supplies words that are not part of, Section 1101-A. 1 Pa.C.S. §§ 1903(a), 1923(c). "Provide for" is a

---

[44] There is a genuine issue of fact regarding the permanency of certain kinds of papers, particularly thermal paper, which is "notorious" for becoming "unreadable in a matter of weeks." (R. 894a). The lower court found that Petitioners' evidence was "too vague and non-specific to declare as a matter of law that vote records printed on thermal paper are not permanent." Ex. A at 14. But even if it were right, it erred in later entering summary judgment ***against*** Petitioners.

[45] (R. 894a ("It is quite possible that the printing may be done days later at the county elections office, and may never be done at all."); R. 763a ("DRE systems are capable of producing paper copies of each ballot. Normally this is done, if at all, at the close of voting.")). This is not surprising, as printing a BIR would result in "miles and miles of paper," (R. 3001a-02a (Shamos Dep. at 148-49)), and the Secretary has instructed counties that they need not do so. (R. 1470a).

phrasal verb, the primary meaning of which is that one supplies what is needed.[46] That makes sense. After all, if one ratified a Constitution that was intended to "provide for the common defence," one would understandably be upset if the President took the position that he was obliged to be capable of repelling an invasion but not obliged actually to repel one.

"Provide for" does not invariably mean "capable of providing." At most, the term is ambiguous and should be interpreted in a manner consistent with Section 1101-A's history and purpose. The legislative history confirms that the General Assembly intended that Section 1101-A would operate as a safeguard by providing a recountable record of votes, not just that they be capable of providing a printout of electronic data that had already been counted. *See supra* VII.A.1. The legislature did not want EVSs to have the same defect as the lever machines they would replace, *see supra* V.C.I., and did not sanction machines that would allow votes to be irretrievably lost if for whatever reason they failed during an election.[47]

But even if "provide for" does mean only 'capable of providing,' it is not enough that an EVS be capable of printing a piece of paper. Rather, an EVS would

---

[46] *See* Richard A. Spears, Ph.D., McGraw-Hill's Dictionary of American Idioms and Phrasal Verbs 520 (2005) (defining "provide for someone or something" as "to supply the needs of someone or something"); The American Heritage Dictionary of Phrasal Verbs 260 (2005) ("provide for. 1. To supply someone or something with basic necessities, as food, shelter, and clothing: ... 2. To take measures in preparation for something....").

[47] This is not conjecture. On the contrary, it happened in Berks County in 2005 when a "failure to use the system in a prescribed manner resulted in a loss of votes," (R. 887a, 1014a), and in North Carolina in 2004. Email from David Eckhardt to Pennsylvania Department of State dated Aug. 25, 2006, *at* http://www.cs.cmu.edu/~davide/voting-machines/Plan_2006-08-25.html.

have to print "a record of each vote cast" that "serves the purposes of the Election Code," one of which is that the record "be available ... for purposes of recounts." Ex. A at 11. And the paper a DRE spits out hours after a vote is cast will never be able to serve that purpose.

For the same reason original electronic data are not a recountable "record," neither is a copy of it. A BIR is an arguably permanent copy of impermanent data that was alterable at any time until printing. At best, they are identical copies that are no more reliable than the original data.[48] At worst, they are not even that. Either way, the copy is no more software independent than the original, and like the original there is no way to say with any confidence that it is actually a "record" of a vote.[49] As Judges McCullough and Pelligrini found, because electronic data are subject to undetectable alteration, making "'print-outs' after the fact does not create a 'permanent physical record.'" Ex. A, Dissent at 2. It follows that the lower court misread Section 1101-A and should be reversed.

---

[48] The Secretary's expert conceded that, "if a physical record of any type is generated from inaccurate or altered data it cannot reflect the original data." (R. 718a). She also agreed that, "[i]f the original is damaged, corrupted, or tampered with, the subsequent copy will reflect the altered information." (R. 427a).

[49] (R. 1005a ("[P]rinting out these ballot images at the end of the day would [not] yield the desired permanent physical record ... if the electronic ballot images were recorded incorrectly or altered during the day.")).

C. DREs Do Not "Preclude Every Person From Tampering With The Tabulating Element" As Required By Section 1107-A (Count II)

Section 1107-A requires that EVSs "preclude every person from tampering with the tabulating element." Section 1107-A, 25 P.S. § 3031.7(16)(iii), (17)(i). DREs do not do that: the record shows that tampering could happen during a live election and, although she argued there was no evidence it had actually happened yet, the Secretary did not dispute that it could. The lower court entered summary judgment against Petitioners anyway, finding that "a mere possibility of a security breach is not alone sufficient to warrant overriding the Secretary's determination to certify the systems." Ex. C at 8. That was an error of law for several reasons, not the least of which being that it overrides the ***General Assembly's*** determination that a possibility of tampering ***is*** sufficient to decertify a system.

1. It Is Possible To Tamper With DRE Tabulating Elements

DREs do not prevent tabulation tampering. On the contrary, there are many ways to affect an election by tampering. For example:

- Dr. Jones testified that it would be possible to inject malicious code into a DRE in order to change its tabulation of votes. (R. 903a ("[T]he key security vulnerabilities required to permit construction of a virus are present.")).
- The Princeton Report found that the AccuVote-TS was susceptible to tabulation tampering: "Malicious software running on a single voting machine can steal votes with little if any risk of detection." (R. 3266a).
- The report also concluded that anyone who has physical access to a voting machine or to a memory card (that will later be inserted into a machine) can install this malicious software using a simple method that

takes less than a minute. In practice, poll workers and others often have unsupervised access to the machines." *Id.*

- The AccuVote-TS machines are also susceptible to viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre and post-election activity. *Id.*

- The Brennan Report identified 35 possible attacks on DREs and noted that "the least difficult attacks against DREs without VVPAT involve inserting Software Attack Programs into the DREs." (R. 3162a).

- Dr. Jones opined that the PEB component of the iVotronic (the device upon which most of the iVotronic's security rests) allows tampering with the tabulating element. (R. 3607a-08a).

Petitioners' experts testified that these vulnerabilities could be exploited in live elections. Dr. Jones opined that "[t]hese defects are not merely of theoretical interest" and have been "tested in a way that could be used to corrupt an election." (R. 3609a; *see also* R. 3611a ("In some cases, as with the vulnerabilities of the ES&S iVotronic PEB interface, there are no feasible procedural defenses. The only procedure that could prevent a voter from attacking an iVotronic through the PEB interface involve [sic] violation of the voter's right to privacy in the voting booth.")). Similarly, Dr. Lopresti opined that it was possible that these security vulnerabilities "could actually happen in Pennsylvania in an election." (R. 3826a). The Secretary's expert admitted that, if successful, these attacks would alter votes. (R. 3010a (Dep. 181:12-182:15)).

2. The "Mere Possibility" Of Tampering With Tabulating Elements Is Enough To Warrant Decertification

The lower court entered judgment against Petitioners because it found that they "can establish no more than that a possibility exists that the challenged DREs could in theory be subject to tampering or human error," the implication being that Petitioners were required to prove that tampering had happened in a live election. Ex. C at 6. That standard finds no support in Section 1107-A's plain language or legislative history.

a. The Lower Court Ignored Section 1107-A's Plain Language

The lower court did not squarely address Section 1107-A's plain language, which says that all EVSs "shall preclude every person ... from tampering with the tabulating element." 1107-A(16)(iii); 1107(A)(17)(i). That language is clear; "shall" is obligatory and "preclude" and "every person" are absolute. Although the lower court referred to this as the "tamper-proof" requirement (Ex. C at 4), it did not meaningfully address the unambiguous, unqualified nature of the language, let alone the rule that "election laws must be strictly construed to prevent fraud." *Shambach,* 577 Pa. at 392, 845 A.2d at 798.

b. The Lower Court Ignored The Legislative History

The lower court also failed to consider the significant legislative history, which confirms that EVS security was a critical concern of the General Assembly. *See supra* Section VII.A.1. Section 1107-A was meant to create "as much security

check as possible" because of concerns about "the possibilities of fraud" that "has not been discovered" and "could be impossible to detect." (R. 2910a-13a). Requiring Petitioners to prove more than a "possibility" of fraud contradicted the legislature's expressed intent.

It is worth noting that the General Assembly's concerns about "possible" but unproven fraud were not unusual. Rather, they were shared by many who were familiar with computers—including the Secretary's own expert witness, who at the time had said "[t]here is danger in allowing machines to choose candidates that the voter has not himself voted for." (R. 1486a (Shamos Memo)). In 1986, Dr. Shamos testified before the Texas House Committee on Elections that there was a "possibility ... of tampering with elections on a truly large scale, as a national scale. An errant programmer, tainted executive could theoretically influence or determine the outcome of a majority of the election precincts in the United States. These problems to me are of a nightmarish proportions [sic]. The possibility of manipulation on such a grand scale does not exist with paper ballots or with lever machines." (R. 3331a).[50] He also cautioned that tampering could be undetectable.

---

[50] *See also* Aviel D. Rubin, Ph.D., *Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting* (2006) (explaining "wholesale fraud verses retail fraud. With the stakes so high, we have to assume that clever and resourceful people will attempt to subvert the process. It has happened too many times before, and will happen again. It isn't feasible to stuff ballot boxes across the entire country, or even in several adjacent polling places. But when computers running exactly the same software are used in ever-larger geographical areas, a bug in the code, whether inadvertent or placed there intentionally, could corrupt the entire outcome of an election, especially when the margins of victory are as narrow as they have been....").

For example, he gave an interview in which he "emphasize[d] the ease of concealing theft by computer without a trace"; characterized local elections as "very vulnerable to fraud"; and regarded the "theft of the Presidency by computer as entirely possible." (R. 2927a). As he put it, "[c]omputerized vote-counting doesn't occur in the light of day, it occurs inside silicon in a little black box. That box is completely under the control of the vender, and if anything wrong happens we might never find out." (R. 2947a). It was these very concerns that caused the General Assembly to require that EVSs preclude tampering—something the challenged DREs simply do not do.

c. The Lower Court Confused or Conflated Section 1107-A With Other Parts of the Election Code

The lower court found that "Petitioners have come forward with no evidence that the challenged machines fail to accurately record votes ***when properly used***." Ex. C at 6 (emphasis added). But what they do "when properly used" is irrelevant, as there is no such language in subsections (16)(iii) or (17)(i). Nor would one expect there to be, given the General Assembly's concerns about election fraud.

The General Assembly could easily have inserted qualifying language into subsections (16)(iii) or (17)(i) if it had wanted to. Indeed, there is such language elsewhere in Section 1107-A, for example in subsection (13), which requires that, "when properly operated," an EVS "records correctly and computes and tabulates accurately every valid vote registered." Including such language in subsection (13)

and excluding it from subsections (16)(iii) or (17)(i) shows that the legislature meant for the latter to be unqualified. *Fonner*, 555 Pa. at 378, 724 A.2d at 907. The lower court's contrary interpretation was wrong as a matter of law.

Similarly, the lower court conflated subsections (16)(iii) or (17)(i) with subsection (11), which requires that EVSs be "capable of" accurate tabulation. The lower court held that "the possibility that tampering can produce inaccuracy does not render the DREs incapable of the absolute accuracy required under the Election Code." (Ex. C at 6). But "capability" and "accuracy" appear nowhere in subsections (16)(iii) or (17)(i). They are different provisions that use different language with different meanings.

Finally, the lower court may have confused subsections (16)(iii) and (17)(i) with subsection (12), which requires "acceptable ballot security procedures" to "prevent tampering with or substitution of ballots." 25 P.S. § 3031.07(12). Whereas subsection (12) arguably affords the Secretary a degree of discretion,[51] subsections (16)(iii) and (17)(i) are drafted in absolute terms that do not.

---

[51] That is not to say, however, that subsection (12) has been satisfied here. On the contrary, the record reveals several security vulnerabilities that allow ballot tampering during an election. *See supra* Section V.C.4. At a minimum this record creates a genuine issue of material fact regarding whether the Secretary discharged her duty to examine systems for compliance with subsection (12) and whether her definition of "acceptable" was arbitrary and capricious for excluding known vulnerabilities.

d. The General Assembly's Security Standard Is Neither Uncommon Nor Unreasonable

The lower court rejected the General Assembly's security standard because it thought that, "[i]f the mere possibility of such error were considered sufficient to bar use of a voting system then we would be left with none." Ex. C at 8. But this case concerns a subset of EVSs, not "voting systems" generally. EVSs are subject to stricter security standard than any other voting systems because the risks from electronic fraud are broader. If DREs do not satisfy that stricter standard, that does not mean we will be "left with no[]" other way to vote. On the contrary, counties could adopt EVSs not challenged here, including optical scan systems that create a recountable record of each vote as it is cast.

Moreover, the legislature's standard is neither uncommon nor unreasonable. To be sure, new and unexpected ways to hack into computers will always arise. EVSs need not prevent exploits that are built on theory but have no way of implementation, and the Secretary need not withhold certification because someone somewhere might someday develop something new. But that does not mean she can tolerate vulnerabilities that are documented in scientific literature and demonstrated in simulated elections, or that she can grant certification (or deny decertification) because she is not troubled by the "mere possibility" of its being exploited. Responsible governments and businesses take steps to respond to new security threats as they arise. Even the Secretary's expert said that that would not

be an impossible standard to satisfy.[52] More to the point, that is the standard the legislature mandated in order to protect a constitutionally protected right. *See* Section 1105-A, 25 P.S. § 3031.5(c) ("if ... it shall appear that the system ... does not meet the requirements hereinafter set forth, the approval of that system shall forthwith be revoked.").

D. The Secretary Failed To Use Testing Procedures That Ensure That DREs Prevent Tampering With Tabulating Elements and Ballots as Required By Section 1105-A (Counts III and VII)

Section 1105-A requires that the Secretary "shall examine the [EVS]" to ensure that it "meets all of the requirements hereinafter set forth," which includes the requirement that it preclude tampering. Section 1105-A, 25 P.S. § 3031.5(b). The lower court found that the Secretary "properly exercise[d] her discretion," that courts cannot "prescribe the best way for [her] to perform her duties," and that Petitioners did not prove that her testing "create[d] more than a mere possibility of error in recording and tabulating votes." Ex. C at 5, 8. That was an error of law.

The Secretary did not do even the minimum that would have been required to make an informed certification decision. On the contrary, her testing was so

---

[52] (R. 861a ("When a problem arises that appears to require attention, the standards should be upgraded at the earliest opportunity consistent with sound practice. If this means that voting machines in the field need to be modified or re-tested, so be it.").

superficial that it rendered the recent reexamination invalid as based on a mistaken understanding of her duties and an arbitrary exercise of discretion.[53]

The lower court did not deal with the deficiency in the examination process as an independent claim. Rather, it conflated that claim with the claims concerning whether the DREs were in fact deficient: "the present cause of action fails nonetheless because the experts have failed to establish that the Secretary's testing procedures and the DREs that she certified create more than a mere possibility of error in recording and tabulating votes." Ex. C at 8. This is a critical error. Voters are entitled to an examination that will allow the Secretary to determine, in the exercise of her discretion, whether the system protects their fundamental constitutional rights. Moreover, the lower court wrongly required Petitioners to "establish" or prove their case, but at the summary judgment stage they need only show a dispute of material facts as to whether the Secretary abused her discretion by not even investigating whether known vulnerabilities had been fixed or were so insignificant a risk that they could be ignored. Willful blindness is not an adequate basis for exercising discretion.

An "examination" to determine whether an EVS "meets all of the requirements" of the Election Code cannot refuse to assess known vulnerabilities.

---

[53] The Secretary's original testing was similarly superficial. *See supra* Section V.C.2. Indeed, two of the originally certified systems (the Unilect Patriot and the AVS WinVote) were eventually decertified for failures to satisfy provisions of the Election Code that had been "overlooked" during the original certifications. (R. 890a (Newkirk Dep. at 321); R.1241a).

Yet that is just what the Secretary did. The reexamination by Mr. Cobb can only be called superficial. *Supra* Section V.C.4. Although the Secretary's own expert had testified how inadequate ITA testing was, the Secretary and her reexaminer relied exclusively on the ITA qualifications issued in 2005 and 2006 to find that the DREs satisfied the Election Code in 2012. (R. 1950a, 2061a, 2179a, 2292a, 2403a, 2513a). As Petitioners' expert noted, "[a]ll of the voting system certifications that are the subject of this case were produced by that flawed [pre-2007 ITA] system." (R. 900a). Mr. Cobb made no meaningful attempt to test security or review any of the well-known recent studies to determine if the vulnerabilities they revealed continued to exist.[54] Even Dr. Shamos understood that "the evidence adduced by California and Ohio should be considered by the Secretary." (R. 756a; *see also* R. 767a). Yet the Secretary all but instructed her reexaminer to ignore them.

The failure to examine the DREs' vulnerability to tampering when there were well-reported studies establishing some level of vulnerability renders meaningless the Secretary's certification that the machines comply with the

---

[54] And when his examination did discover a vulnerability, he did even require remediation. During the reexamination of the iVotronic for example, Mr. Cobb observed that the lock placed over the serial port and compact flash did not prevent access to the compact flash. (R. 3890a). He admitted that it was possible to access and replace the flash card in order to upload a virus or swap election results. (R. 3890a). Although he recommended that a different lock be used, and recognized the potential resulting security vulnerabilities, he did not recommend conditioning approval of the iVotronic system on using a different type of lock. (R. 3890a).

Election Code. Unfortunately, she and her examiner do not know whether that is true or not, and her certification—in light of her failure to investigate known vulnerabilities—must be deemed an arbitrary exercise of discretion. *Cf. Scenic Hudson Pres. Conference v. Fed. Power Comm'n*, 354 F.2d 608, 612 (2d Cir. 1965) ("If the Commission is properly to discharge its duty [to determine if granting a license is consistent with its statutory duty], the record on which it bases its determination must be complete. The petitioners and the public at large have a right to demand this completeness"). The Secretary has either misunderstood her duty to assess the compliance of the machines or has abused her discretion by failing to acquire the knowledge necessary to exercise her discretion in an informed and meaningful manner.[55]

The Secretary claims that mandamus cannot be used to tell her how to examine an EVS. But the case law is clear that mandamus can direct performance of a required act, which is an ***examination*** that will ***determine if*** the machines comply with the complex statutory requirements that protect fundamental rights. The Secretary has not been authorized to say "no examination is necessary because I will certify the machines no matter how they function." Nor can she be permitted to say "I will certify the machines even though I do not know how they function

---

[55] "Acceptable ballot security" must be read in light of the Constitutional values the legislature was protecting: the right to have one's vote counted as cast. *Cf. Robinson Township v. Pa.* (63 MAP 2012, S.Ct. Pa) at 130-33 holding statutory standard for granting waivers must take into account and be compatible with underlying constitutional provisions.

because my examiner did not read readily available studies about how they function or ask if problems which have led to de-certifications in other states exist here." Her unilateral declaration that she has conducted an examination does not conclude the issue. That is too much like Humpty Dumpty declaring that a word "means just what I choose it to mean." *Through the Looking Glass*, Chap. 6.

As this Court said in a case involving the Pennsylvania Game Commission, "[t]he Commission does not have the power to redefine its authority at will; the courts are an appropriate destination, and mandamus an appropriate remedy, to direct the Commission to comply with its statutory mandate to the extent it misapprehends it." *Seeton v. Pa. Game Comm'n,* 594 Pa. 563, 574, 937 A.2d 1028, 1034 (2007). The duty to conduct a meaningful examination in order to knowingly certify whether the machine complies with legislative standards is particularly appropriate and important when the Secretary takes the position that the law does not require any independent record of votes cast which can be turned to if an unanticipated event occurs. Because the harms—votes irretrievably lost or undetectably changed—to the fundamental constitutional right to vote are so great, the corresponding duty to know whether the risk has been addressed should be equally great. The lower court essentially said that there was no middle ground between requiring perfection and giving *carte blanche* for however superficial an examination the Secretary chooses to conduct. That is not the law, and it makes a

mockery of the legislative branch's enumeration of particular requirements that it wanted the executive branch to ensure were satisfied in order to protect voters' fundamental right to vote.

The Election Code requires that the Secretary test for all of its requirements, including those pertaining to security and tampering. The Secretary did not do so, and the lower court erred in entering judgment against Petitioners on this claim.

E. The Commonwealth Court Erred in Entering Judgment Against Petitioners on their Constitutional Claims (Counts VII, IX & X)

Petitioners have advanced three claims under the Pennsylvania Constitution, specifically under Article I, section 5 (Count VIII), Article I, section 26 (Count IX), and Article VII, section 6 (Count X). These claims turn on the undisputed fact that DREs cannot verify voter intent but other EVSs can. Nevertheless, the Secretary has certified these unverifiable machines without asserting a compelling reason. Nowhere in her examinations or certifications is there any sign that she was cognizant of the need to prevent infringement of the fundamental voting rights enshrined in our Constitution. The lower court did not address Petitioners' constitutional claims at all, reasoning that Petitioners had not shown that DREs are insecure and inaccurate. In doing so, it ignored the constitutional mandate of preventing any interference with the right to vote and improperly deferred to a certification that was not faithful to our constitutional values.

1. The Right To Vote Is An Inherent Right Of Mankind And Must Remain Inviolate

The parties do not dispute that the right to vote is fundamental. *See, e.g., Applewhite v. Commonwealth*, 54 A.3d 1, 3 (Pa. 2012) ("The parties to this litigation have agreed that the right to vote in Pennsylvania, as vested in eligible, qualified voters, is a fundamental one.") Unlike the U.S. Constitution, our Constitution explicitly recognizes the right to vote in two separate sections. Pa. Const. art. I, § 5 ("[N]o power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage."); *id.* at art. VII, § 1 ("Every citizen twenty-one years of age, possessing the following qualifications, shall be entitled to vote at all elections subject, however, to such laws requiring and regulating the registration of electors as the General Assembly may enact."). It is not surprising, then, that our Supreme Court has called the right to vote "sacred." *Page v. Allen*, 58 Pa. 338, 347 (1868). The U.S. Supreme Court has similarly said that "[n]o right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *Wesberry v. Sanders*, 376 U.S. 1, 17 (1964).

Just as the right to vote cannot be denied outright, neither can it be "destroyed by alteration of ballots, nor diluted by ballot-box stuffing." *Reynolds v. Sims*, 377 U.S. 533, 555 (1964). "[I]ncluded within the right to [vote] ... is the

right of [] voters within a state to cast their ballots and have them counted." *U.S. v. Classic*, 313 U.S. 299, 315 (1941); *see also Reynolds*, 377 U.S. at 555 ("the right of suffrage can be denied by a debasement or dilution of the weight of a citizen's vote just as effectively as by wholly prohibiting the free exercise of the franchise."). Thus, the fundamental right to vote includes the right to have one's vote counted as cast. *See Black v. McGuffage*, 209 F. Supp.2d 889 (N.D. Ill. 2002) (holding that plaintiffs stated an equal protection claim where they alleged that votes in some counties were less likely to be counted than votes in other counties).

This Court recently confirmed Pennsylvania's strong textual guarantee of fundamental rights such as the right to vote. In *Robinson Twp., Washington Cty. v. Commonwealth*, No. 63 MAP 2012 (Pa. Dec. 19, 2013), it explained that "Article I is the Commonwealth's Declaration of Rights, which delineates the terms of the social contract between government and the people that are of such 'general, great and essential' quality as to be ensconced as 'inviolate.'" *Id.* at 67. State regulation of inviolate rights "'are to be subordinate to the enjoyment of the right, the exercise of which is regulated. The right must not be impaired by the regulation. It must be regulation purely, not destruction.'" *Id.* at 60 n.31 (quoting *Page*, 58 Pa. at 347).

In *Robinson Township*, this Court held that courts "have an obligation to make some independent assessment of state constitutional provisions." *Id.* at 62. It explained that courts are "obliged to weigh parties' competing evidence and

arguments, and to issue reasoned decisions regarding constitutional compliance by the other branches of government." *Id.* at 77. It is thus necessary for a court to "pass upon a constitutional challenge ... not by measuring the wisdom of the means chosen ... but by measuring the [action] against the relevant constitutional command." *Id.* at 123. Here, an assessment of the constitutional validity of the Secretary's actions is required because the constitutional charge must be respected by all levels of government. *Id.* at 75. Thus, the lower court erred when it failed to analyze the claims that certifying the challenged DREs violated the Constitution. When properly measured against the textual guarantees of the right to vote, the Secretary's actions fall far short.

2. The Certification of Unverifiable Systems When Verifiable Systems Exist Is Inconsistent With The Constitutional Mandate

It is undisputed that no one can know whether the challenged DREs correctly captured voter intent. Yet the Secretary permitted counties to use them. In so doing, she contradicted both the legislative requirements that the General Assembly dictated and the constitutional obligations that state action "shall [not] interfere to prevent the free exercise of the right of suffrage" and that neither the Commonwealth nor any political subdivision "shall deny to any person the enjoyment of any civil right." Art. I, §§ 5 & 26. Just as the legislature may not interfere with the right of suffrage directly, it may not do so indirectly by making the right more susceptible to interference by others. For this reason, the legislature

mandated that electronic voting systems provide for a permanent physical record, that they be subjected to an automatic recount, and that they preclude tampering with tabulating elements and ballots. *See supra.*

The certification of DREs that make it easier for voting rights to be interfered with and make it harder for such interference to be detected is inconsistent with the "inviolate" values embodied in Article I, sections 5 and 26. Regulating voting cannot occur at the expense of unreasonably burdening voting. *Robinson Twp.*, slip op. at 79 (recognition of environmental rights as inviolate necessarily implies that state-sanctioned economic development cannot take place at the expense of an unreasonable degradation of the environment). The Secretary has turned the natural order of rights and regulation on its head. Rather than the regulation being "subordinate to the enjoyment of the right," *Page*, 58 Pa. at 347, the Secretary's action unreasonably impairs its enjoyment.

This Court should apply strict scrutiny to the Secretary's certification of unverifiable systems because those systems burden "the most treasured prerogative of citizenship." *Appeal of Norwood*, 382 Pa. 547, 549, 116 A.2d 552, 553 (1955); *see also James v. SEPTA*, 505 Pa. 137, 145, 477 A.2d 1302, 1305-06 (1984) ("[W]here ... a fundamental right has been burdened, another standard of review is applied: that of strict scrutiny."). Strict scrutiny requires that the Secretary demonstrate that the continued use of unverifiable DREs is "narrowly tailored to

serve a compelling state interest." *DePaul v. Commonwealth*, 600 Pa. 573, 585, 969 A.2d 536, 543 (2009). Nowhere in the record does the Secretary articulate any interest, let alone a compelling interest, that is served by keeping unverifiable DREs in service. Nor has she urged that unverifiable DREs are necessary to protect the integrity of the democratic process. Her silence is especially significant in light of the fact that other states have jettisoned these same DREs for systems that create software-independent records.

Further, the Secretary cannot demonstrate that the use of unverifiable DREs is the least restrictive means of furthering any purported governmental interest. *See Ins. Adjustment Bureau v. Ins. Comm'r*, 518 Pa. 210, 224, 542 A.2d 1317, 1324 (1988). Given the certification of verifiable EVSs that do not interfere with the fundamental right to vote, the Secretary's certification of unverifiable DREs does not satisfy strict scrutiny.

The Secretary's and the lower court's interpretation of the Election Code permits the use of voting systems that interfere with the fundamental right to vote. "[S]tatutes are to be construed whenever possible to uphold their constitutionality." *In re William L.*, 477 Pa. 322, 329, 383 A.2d 1228, 1231 (1978); *accord* Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 247 (2012). To faithfully carry out Article I's command that the right to vote shall not be interfered with, the Election Code should be interpreted to require a verifiable

record. The lower court's ruling presents a constitutional issue that cannot be cured with the rationalization that "no voting system is perfect." To the contrary, no voting system shall "prevent the free exercise of the right of suffrage."

Just as the Secretary failed to examine whether the DREs satisfied the Election Code, the lower court failed to apply any degree of scrutiny—let alone the strict scrutiny that is required—to whether the Secretary satisfied the Constitution. It is the role of the courts to protect these constitutionally secured rights against executive action, including acts of omission, which disregard their inviolate stature. This Court may engage in such an analysis because the challenge to the constitutionality of the Secretary's action poses a question of law, the review of which is plenary and non-deferential. *Robinson Twp.*, slip op. at 59. When it is measured against the Constitution's commands, the Secretary's certification of unverifiable systems impermissibly burdens the right to vote.

3. The Secretary's Creation of Different Classifications Of Voters Cannot Survive Scrutiny Because It Is Not Narrowly Tailored To Advance A Compelling State Interest

The Secretary's creation of two distinct classifications of voters runs afoul of Article VII, section 6, which requires that "All laws regulating the holding of elections by the citizens ... shall be uniform throughout the state." Those who vote on systems without software-independent records of their intent are harmed because they have a right to have their vote weighted properly without dilution or

discount. *Reynolds*, 377 U.S. at 555. Letting some voters use unverifiable DREs while others use systems that create a software independent record of voter intent must be strictly scrutinized to determine if such classifications violate the uniformity required.

At least one court has recognized a constitutional injury for voters who are forced to vote on systems with a higher probability that one person's vote will not be counted as a result of the type of voting system used. *Black*, 209 F. Supp.2d at 895. The *Black* court held that the state may not by "arbitrary and disparate treatment, value one person's vote over that of another." *Id.* at 898. Moreover, the fact that local authorities select a voting system from among a variety of systems did not insulate the state from a constitutional violation. Rather, that choice was the crux of the problem because "some authorities will choose a system with less accuracy than others. As a result, voters in some counties are statistically less likely to have their votes counted than voters in other counties in the same state in the same election for the same office." *Id.* at 899. In denying a motion to dismiss, the court held that "[a]ny voting system that arbitrarily and unnecessarily values some votes over others cannot be constitutional." *Id.* It follows that creating two classes of voters—one whose votes can be verified and one whose votes cannot—violates Art. VII, section 6.

VIII. CONCLUSION

Petitioners respectfully request that this Court reverse the lower court and instruct it to enter judgment in favor of Petitioners.

Respectfully submitted,

DATED: January 6, 2014

Michael P. Daly (Id. No. 86103)
Meredith N. Reinhardt (Id. No. 93504)
Katie L. Bailey (Id. No. 308748)
David A. Solomon (No. 312401)
Garrett D. Trego (No. 314496)
Drinker Biddle & Reath LLP
One Logan Square, Suite 2000
Philadelphia, PA 19103-6996

Marian K. Schneider (Id. No. 50337)
Law Office of Marian K. Schneider
295 E. Swedesford Road, #348
Wayne, PA 19087

Michael Churchill (Id. No. 4661)
Benjamin D. Geffen (Id. No. 310134)
Public Interest Law Center of Philadelphia
United Way Building, 2nd Floor
1709 Benjamin Franklin Parkway
Philadelphia, PA 19103

Counsel for Appellants

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing document complies with the 14,000 word limit established by Pa. R.A.P. 2135.

DATED: January 6, 2014

Garrett D. Trego

PROOF OF SERVICE

I hereby certify that I am this day serving the foregoing document upon the following by First Class Mail, postage prepaid, which satisfies the requirements of Pa. R.A.P. 121 and 122:

Steven Edward Bizar
Robert J. Fitzgerald
Shawn N. Gallagher
Buchanan Ingersoll & Rooney PC
Two Liberty Place, 50 S. 16th St.
Philadelphia, PA 19102-2555

Steven V. Turner
Kathleen M. Kotula
Office of General Counsel
Commonwealth of Pennsylvania
301 North Office Building
Harrisburg, PA 17120

Attorneys for Appellee

DATED: January 6, 2014

Garrett D. Trego

EXHIBIT A

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	No. 442 M.D. 2006
	:	Argued: November 16, 2011
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

BEFORE: **HONORABLE BONNIE BRIGANCE LEADBETTER,** President Judge
HONORABLE BERNARD L. McGINLEY, Judge
HONORABLE DAN PELLEGRINI, Judge
HONORABLE RENÉE COHN JUBELIRER, Judge
HONORABLE ROBERT SIMPSON, Judge
HONORABLE MARY HANNAH LEAVITT, Judge[1]
HONORABLE PATRICIA A. McCULLOUGH, Judge

OPINION BY
PRESIDENT JUDGE LEADBETTER[2] **FILED: August 29, 2012**

---

[1] This case was argued before an en banc panel of the Court that included former Judge Johnny J. Butler. Because Judge Butler's term on the Court ended January 2, 2012, this matter was submitted on briefs to Judge Leavitt as a member of the en banc panel.

[2] This case was assigned to President Judge Leadbetter on or before January 6, 2012, when she completed her term as President Judge.

Petitioners, twenty-four individual voters,[3] move for partial summary judgment in this original jurisdiction matter filed against the Secretary of the Commonwealth (Secretary). For the reasons that follow, we deny the motion.[4]

In late 2006, Petitioners filed a ten-count petition for review against the Secretary, seeking declaratory relief and an order directing the Secretary to decertify the Direct Recording Electronic voting systems (DREs) used in Pennsylvania, establish uniform testing criteria that complies with the Pennsylvania Election Code,[5] and reexamine the DREs as previously requested. As noted in the petition, the Secretary certified various DREs for use in Pennsylvania elections.[6] DREs do not use a document/paper ballot in the vote process. Rather, DREs display ballots electronically on an interface screen and allow a voter to make choices with a push button, dial or touch screen and then cast his or her vote. DREs record each vote as digital markings in various forms of internal memory; they do not produce a contemporaneous external paper record of a voter's selections/vote. In addition, most of the DREs also store the vote records on

---

[3] Specifically, Petitioners are Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs–Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero and Jeanne Zang.

[4] This is the second time this case is before us. Previously, we denied the Secretary's preliminary objections to the petition for review. *See Banfield v. Cortes*, 922 A.2d 36 (Pa. Cmwlth. 2007) (en banc).

[5] Act of June 3, 1937, P.L. 1333, *as amended*, 25 P.S. §§ 2600-3591.

[6] The Secretary has certified the following DREs: the AVC Edge II and the AVC Advantage, made by Sequoia Voting Systems, Inc.; the iVotronic, made by Elections Systems & Software, Inc.; the eSlate, made by Hart InterCivic, Inc.; the ELECTronic 1242, made by Danaher Industrial Controls; the AccuVote TSX, made by Diebold Election Systems, Inc.; and the WINvote, made by Advanced Voting Solutions. The WINvote was subsequently decertified. DREs have been used in Pennsylvania since 2006.

removable memory devices, such as flash drives or memory cards.[7] Finally, the DREs are capable of printing the stored vote data on paper; some systems print vote records on thermal paper, similar to that used for receipts, and others print on a full page. Pertinent to Petitioners' claims and the main concern underlying their legal arguments is that because the voting systems do not produce a contemporaneous paper record of each vote cast, voters cannot verify that their votes were recorded accurately and election officials have no independent physical record to use for auditing DRE vote counts. According to the petition for review, although Petitioners have satisfied the requirements set forth in the Election Code for the Secretary to reexamine the previously certified DREs, the Secretary has improperly denied multiple requests for reexamination.[8]

The Secretary filed preliminary objections to the petition, which were overruled by opinion and order of this court. *See Banfield v. Cortes,* 922 A.2d 36 (Pa. Cmwlth. 2007) (*en banc*), permission to appeal denied by Supreme Court order dated December 16, 2008 (70 MM 2007). Following responsive pleadings and discovery, Petitioners filed the present motion seeking judgment in their favor as to Counts I, IV, VI, IX, and X, primarily on the basis that, inasmuch as there is no dispute regarding certain technical attributes of the DREs, the DREs fail to

---

[7] To illustrate, according to Petitioners, the Danaher ELECTronic 1242 stores vote data in three separate RAM locations and on a memory cartridge containing "three distinct memories for storing data: one EPROM and two EEPROMS." Petitioners' memorandum of law in support of motion for partial summary judgment at 13.

[8] For instance, according to the petition, Alan Brau, by letter dated March 7, 2006, asked the Secretary to reexamine one of the certified DREs. Brau enclosed a check in the requisite statutory amount of $450, and provided the statutorily-required signatures of ten qualified electors. According to the petition, the former Secretary denied Brau's request shortly thereafter, stating that he was not aware of any changes to the subject DRE. The petition avers that the Secretary received three other similar requests and all were denied for the same reason.

comply with specific provisions of the Election Code, thereby entitling Electors to judgment as a matter of law.[9] Specifically, Petitioners aver that: (1) the DREs fail to comply with Section 1101-A,[10] 25 P.S. § 3031.1 (defining "electronic voting system" as a system that, *inter alia*, "provides for a permanent physical record of each vote cast") (Count I); (2) the DREs fail to comply with Section 1117-A,[11] 25 P.S. § 3031.17 (requiring a statistical recount of random sample of ballots using "manual, mechanical or electronic devices of a type different" than those used for election) (Count IV); and (3) the Secretary's failure to reexamine the DREs upon request violates Section 1105-A,[12] 25 P.S. § 3031.5 (requiring Secretary to reexamine electronic voting system upon request) (Count VI). Petitioners further contend that the Secretary's certification of the specified DREs violates Article I, § 26 of the Pennsylvania Constitution (equal protection) (Count IX), and Article VII, § 6 of the Pennsylvania Constitution (uniformity) (Count X).[13]

Prior to addressing the arguments, it is helpful to note the relevant statutory provisions pertaining to electronic voting systems like the DREs at issue here. The Election Code defines an "electronic voting system" (or EVS) as "a system in which one or more voting devices are used to permit the registering or

---

[9] The Secretary has filed her own application for summary relief. In scheduling argument on the instant application, the court directed that all other matters, including the Secretary's application, be held in abeyance. *See* order dated August 17, 2011.

[10] Added by the Act of July 11, 1980, P.L. 600.

[11] Added by the Act of July 11, 1980, P.L. 600.

[12] Added by the Act of July 11, 1980, P.L. 600.

[13] Summary judgment may be granted only in those cases "where the record clearly shows that there are no genuine issues of material fact and that the moving party is entitled to judgment as a matter of law." *P.J.S. v. Pa. State Ethics Comm'n*, 555 Pa. 149, 153, 723 A.2d 174, 176 (1999). Moreover, "[w]hen resolving a motion for summary judgment, the record must be viewed in the light most favorable to the opposing party, and all doubts as to the existence of a genuine issue of material fact must be resolved in favor of the nonmoving party." *Id.*

recording of votes and in which such votes are computed and tabulated by automatic tabulating equipment. The system shall provide for a *permanent physical record* of each vote cast." Section 1101-A (emphasis added). A "voting device" is defined, in turn, as "either an apparatus in which paper ballots or ballot cards are used in connection with an implement by which a voter registers his votes with ink or other substance or by punching, or an apparatus by which such *votes are registered electronically*, so that in either case the votes so registered may be computed and tabulated by means of automatic tabulating equipment." *Id.* (emphasis added). Finally, "automated tabulating equipment" is defined by the Code as "any apparatus which automatically examines and computes votes registered on paper ballots, ballot cards or district totals cards or votes registered electronically and which tabulates such votes." *Id.*

The Secretary must first examine and approve any EVS before any county board of elections may adopt it for use. Sections 1102-A, 1105-A, added by the Act of July 11, 1980, P.L. 600, 25 P.S. §§ 3031.2, 3031.5.[14] In addition, prior to approving an EVS, the Secretary must establish that the system meets the requirements set forth in Section 1107-A, added by the Act of July 11, 1980, P.L. 600, 25 P.S. § 3031.7.[15] The Secretary's approval signifies that "the system so

---

[14] In addition to Secretary examination and approval, the systems are also examined and approved by a federally recognized independent testing authority and must first meet any voting system performance and test standards established by the Federal Government. Section 1105-A(a).

[15] For instance, Section 1107-A requires, *inter alia*, that each EVS: (1) provides for voting in absolute secrecy; (2) permits each voter, at other than primary elections, to vote a straight political party ticket by one mark or act; (3) permits each voter, at other than primary elections, "to vote a ticket selected from the nominees of any and all political parties, from the nominees of any and all political bodies, and from any persons whose names are not in nomination and do not appear upon the official ballot;" (4) if of the type that registers votes electronically, "preclude[s] each voter from voting for more persons for any office than he is entitled to vote for or upon any

(Footnote continued on next page...)

examined can be safely used by voters at elections as provided [in the Election Code] and meets all of the requirements hereinafter set forth [in the Code]." Section 1105-A(b), 25 P.S. § 3031.5(b). Once a county board of elections purchases, leases or otherwise procures electronic voting systems for use in its election districts, the county board of elections provides all the elements of the voting system to the election districts and, among other things, appoints a custodian and deputy custodians, if necessary, to prepare the voting system and its components for use. *See* Sections 1104-A, 1110-A, added by the Act of July 11, 1980, P.L. 600, 25 P.S. §§ 3031.4, 3031.10. Relevant to the instant action, following an election, the county board of elections "as part of the computation and canvass of returns, shall conduct a statistical recount of a random sample of ballots after each election using *manual, mechanical or electronic devices of a type different* than those used for the specific election." Section 1117-A, 25 P.S. § 3031.17 (emphasis added).

We begin with the contention that the DREs fail to "provide for" a permanent physical record of each vote cast. While there is no dispute that the DREs are capable of printing a paper record of the votes cast (discussed more fully below), Petitioners argue that the systems fail to "provide for" the requisite records because they do not automatically create a contemporaneous paper record when

---

(continued...)

question more than once;" (5) if of the type that registers votes electronically, "permits each voter to change his vote for any candidate or upon any question appearing on the official ballot up to the time that he takes the final step to register his vote and to have his vote computed;" (6) "*[p]rovides acceptable ballot security procedures and impoundment of ballots to prevent tampering with or substitution of any ballots or ballot cards*;" and (7) when operated properly, "*records correctly and computes and tabulates accurately every valid vote registered.*" (emphasis added).

each vote is cast. According to Petitioners, the printed vote records that the machines will provide are only generated, if at all, at the close of voting or days later. Petitioners cite to a plethora of dictionary definitions to support their construction that the phrase "provide for" requires the actual provision of the needed item, as opposed to the ability to provide the item at a later time upon request.[16]

The Secretary, on the other hand, relying on her own dictionary references, construes "provide for" to require only the capability of providing the specified item upon demand if needed. Thus, if a DRE can provide the requisite permanent physical records when specifically requested, it qualifies as an EVS as defined by the Election Code. While we do not find the phrase ambiguous, we note that we agree with the Secretary's construction that "provide for" denotes the ability to generate or supply the required records on demand; it does not mean that such records must be generated automatically with each vote cast.[17] If the phrase is

---

[16] As a general rule of statutory construction, "[w]ords and phrases shall be construed according to rules of grammar and according to their common and approved usage...." Section 3 of the Statutory Construction Act of 1972, 1 Pa. C.S. § 1903. Moreover, we note that: "Whenever possible each word in a statutory provision is to be given meaning and not to be treated as surplusage." *Matter of Employees of Student Services, Inc.*, 495 Pa. 42, 52, 432 A.2d 189, 195 (1981). Finally, when statutory language is ambiguous, construction of the language by the administrative body charged with its execution and application is entitled to great weight and deference and will not be disregarded unless clearly erroneous. *In re Thompson*, 896 A.2d 659, 669 (Pa. Cmwlth. 2006).

[17] *See generally*, Webster's Third New International Dictionary at 1827 (1993) (defining "provide" as an intransitive verb as: "**1a**: to take precautionary measures: make provision – used with *against* or *for* . . . < ~ for the common defense – *U.S. Constitution* >);" Oxford Dictionaries Online at http://oxforddictionaries.com/definition/provide?region=us&q=provide+for [defining "provide" as a verb with and without an object, in pertinent part, as: "**2** [no object] (provide for) make adequate preparation for (a possible event); *new qualifications must provide for changes in technology* . . . (of a law) enable or allow (something to be done)];" MacMillan Dictionary at http://www.macmillandictionary.com/dictionary/british/provide-for (defining "provide for" as a

(Footnote continued on next page...)

construed as Petitioners advocate, the word "for" in the phrase "provide for" becomes superfluous.

Next, we must determine whether the DREs create "permanent physical records" of "each vote cast." It is undisputed that the DREs automatically create electronic records of each vote cast and can generate a paper record of each vote cast upon request. The latter records are created using the DRE's cast vote record or ballot image retention (BIR) function; a ballot image of each recorded vote is created and stored in the DRE's electronic memory and can be printed at the close of the election.[18] Respondent's Exhibit (Ex.) 9, Report of Michael I. Shamos, Ph.D., J.D., at ¶ 47; Ex. 25, Permanent Manual Audit Capacity Documentation for Certified DRE Voting Systems, dated April 11, 2006; Petitioners' Ex. 11, Report of Daniel Lopresti, Ph.D. at 4-5; Ex. 7, Report of Douglas W. Jones, Ph.D., at ¶ 34, 35. As noted, the electronic records are stored both on the machines themselves and on removable media, such as flash drives or memory cards.

According to Petitioners, neither the electronic records nor the printed paper records satisfy the requirements of the Code. Construing the permanency specification to mandate a record which remains forever unalterable, Petitioners

---

(continued...)

transitive phrasal verb, in relevant part, as "**2**$_{[\cdot]}$ **provide for something** to make it possible for something to happen in the future *The budget provides for a salary increase after one year.*);" Cambridge Dictionary at http://dictionary.org/dictionary/british/provide-for-sth?q=provide+for+sth (defining "provide for [something]" as "• to make plans in order to deal with a possible event in the future . . . • FORMAL if a law or agreement provides for something, it allows it to happen or exist").

[18] The BIR function is somewhat of a misnomer. Apparently, neither a ballot image nor a reproduction of the visual screen image is actually provided. Rather, "a record of what votes the machine collected from that voter" is provided. *See* Petitioners' Ex. 7, Report of Douglas Jones, Ph.D., at ¶ 56.

first contend that the electronic vote records are not permanent because they are continually subject to change or at risk of alteration, either intentional or unintentional. In support, they note the opinion of their computer science and engineering expert, Daniel Lopresti, Ph.D. According to Dr. Lopresti:

> [DREs] employ computer memory technology to create an "electronic record" which is, by its very nature, freely alterable during the election in ways that are undetectable after-the-fact.
>
> . . . .
>
> [T]he accuracy or permanence of the data stored electronically cannot be guaranteed due to the inherent characteristics of electronic computer memory. All of the forms of computer memory used in the DRE voting system . . . are freely writable under software control for the period of time that the election is taking place. Computer memory can be written or rewritten with incorrect data unintentionally (as a result of software and/or hardware and/or human error) or intentionally (as a result of a malicious attempt to alter the results of an election). Moreover, the act of writing computer memory is in principle undetectable; it leaves behind no physical evidence. This is true even for flash memory modules that contain a manually activated switch or fuse to disable their rewritability at the end of the election; until writability is disabled, typically at the end of the election, the contents of the flash memory may be altered in arbitrary ways. Since even the initial writing of a record into computer memory is accomplished through the use of software and hardware intermediaries, there is no way for a human observer to confirm that what is written is in fact an accurate record of his/her vote.

Petitioners' Ex. 11 at 2-3, 4-5.[19]

---

[19] Petitioners further note in their reply brief that: "[T]he data is freely alterable during the entire course of an election while DREs are operating, meaning that the data purporting to represent the vote of an elector who cast a ballot in the morning is in an alterable (and, thus, impermanent) state until the polls close . . . The proper focus is not on how long data could be or **(Footnote continued on next page...)**

Petitioners also contend that, even assuming that the data is not altered during the course of the election and that the data on electronic media can be retained for years if stored under proper conditions, "there is nothing in the record to suggest that anyone actually **does** that." Petitioners' memorandum of law in support of motion for partial summary judgment at 34 (emphasis in original). According to Petitioners, "the record suggests that counties reuse the same 'removable' memory cards over and over in each election and in doing so destroy any data that may have been stored on them from prior elections." *Id.*[20] Thus, Petitioners' primary concerns are that (1) electronically recorded vote data can be altered during the election without detection,[21] and (2) in practice, the vote records are not permanent because they are not retained.

The Secretary asserts, however, that "permanent" denotes a state of being that is "continuing or enduring without fundamental or marked change," or

---

(continued...)

should be retained, but on whether it is subject to alteration." Petitioners' reply brief at 6 (footnote omitted).

[20] In support, Petitioners note that in the past, the Secretary has directed counties as follows:

> A county board of elections may reuse memory cards for the next election if the county maintains either a printed or electronic copy of the ballot images contained in the system. For Federal elections, a county board of elections must retain these ballot images for 22 months from the date of the election. 42 U.S.C. § 1974. For municipal elections, the county board of elections must retain the ballot images for a [sic] least 20 days, unless ordered otherwise by a court as provided at Section 1230 of the Election Code, 25 P.S. § 3070.

Petitioners' Ex. 42, Directive Concerning the Use, Implementation and Operation of Electronic Voting Systems by the County Board of Elections, dated September 3, 2008, at 5.

[21] Petitioners do not appear to be alone in this regard. In addition to their experts, others have articulated this same concern. *See generally* www.commoncause.org (nonpartisan citizens organization commenting on electronic voting systems).

"stable; that is, it will not change unless some other force acts upon it." Respondent's brief at 24 (quoting in part from the Merriam-Webster Dictionary at www.merriam-webster.com/dictionary/permanent). The Secretary also contends that "permanent" cannot be construed to require a record that is capable of lasting forever in a constant state or one that is immune from alteration or loss as a result of outside actions or forces because such construction would defy reality and is impossible to achieve.

First, we disagree with Petitioners' contention that use of the term "permanent" requires an electronic record that is immune from wrongful or malevolent alteration or destruction or even alteration or destruction resulting from unintentional human error or mishap. As the Secretary notes, any record, whether paper or electronic, is subject to destruction, loss, tampering or wear. We agree with the Secretary that the term must be construed in a manner which serves the purposes of the Election Code.[22] Accordingly, we conclude that a permanent record is one that will remain stable or intact and be available for an indefinite period of time, but at a minimum, twenty days for purposes of recounts, recanvasses,

---

[22] Section 301 of the Civil Rights Act of 1960, 42 U.S.C. § 1974, requires, in pertinent part, that: "Every officer of election shall retain and preserve, for a period of twenty-two months from the date of any general, special, or primary election of which candidates for the office of President, Vice President, presidential elector, Member of the Senate . . . are voted for, all records and papers which come into his possession relating to any application, registration . . . or other act requisite to voting in such election . . . ."

The Election Code, on the other hand, requires that vote records be retained for a shorter minimum period of time. *See, e.g.*, Section 1230, 25 P.S. § 3070 (providing that "voting machines shall remain locked against voting for the period of twenty days next following each primary and election, and as much longer as may be necessary or advisable because of any existing or threatened contest over the result . . . ;" Section 1702(c), 25 P.S. § 3262(c) (requiring in pertinent part that, "[v]oting machines may be recanvassed . . . at any time within twenty days after the date of the primary or election at which they were used.").

litigation, etc., in state-related contests and twenty-two months in federal-related election matters.[23] Immunity from intentional election fraud or unintentional loss or destruction is not a common and approved understanding of the word, nor is it a construction which is necessary to serve the purposes of the Election Code.

Second, to construe "permanent" to denote a vote record immune from human alteration, mishap or loss, renders Section 1107-(A)(11), (12) and (13), 25 P.S. § 3031.7(11), (12), and (13), redundant. Those sections provide, respectively, that in order to be approved by the Secretary, the EVS: "is safely and efficiently useable in the conduct of elections and, with respect to the counting of ballots cast . . . is suitably designed and equipped to be capable of absolute accuracy, which accuracy shall be demonstrated to the Secretary[;]" "[p]rovides acceptable ballot security procedures and impoundment of ballots to prevent tampering with or substitution of any ballots or ballot cards[;]" and "[w]hen properly operated, records correctly and computes and tabulates accurately every valid vote registered." Here, Petitioners' memorandum of law does not point to any undisputed record evidence that demonstrates that an electronic record, which has been created by a EVS meeting all requirements for certification, cannot be accurately retained for time periods mandated by law.

---

[23] "Permanent" has been defined as (1) "continuing or enduring (as in the same state, status or place) without fundamental or marked change: not subject to fluctuation or alteration: fixed or intended to be fixed: lasting, stable," *see* Webster's Third New International Dictionary at 1683; (2) "existing or intended to exist for an indefinite period [*e.g.*,] a permanent structure" or "not expected to change for an indefinite time; not temporary [*e.g.*,] a permanent condition," *see* Collins English Dictionary online at www.collinsdictionary.com/dictionary/english/permanent; and (3) "existing perpetually; everlasting, especially without significant change[,]" or "intended to exist or function for a long, indefinite period without regard to unforeseeable conditions: *a permanent employee; the permanent headquarters of the United Nations*[,]" or "long-lasting or nonfading:[ ] *permanent ink*[,]" *see* Dictionary.com at dictionary.reference.com/browse/permanent?s=t.

We also note that the prospect that some counties may actually reuse the electronic storage media in subsequent elections without preserving a printed copy of the vote data or another electronic copy does not command a different conclusion. The dispositive question is whether the DREs certified by the Secretary provide a permanent record of each vote cast, not whether the machines are being used properly or whether the county boards of elections are properly performing their duties under the Code.

Petitioners also take issue with the permanency of the printed vote records that the DREs can produce.[24] According to Petitioners, many of the DREs print the ballot images and vote records on "receipt-grade, ribbon-like thermal paper," which Petitioners suggest is fragile and prone to fading and deterioration, and, therefore, cannot be considered as a permanent record.[25] In support, they point to, *inter alia*, the opinion of their computer expert, Dr. Jones, who opined as follows:

> Thermal printer paper is notorious for not being very permanent. Anyone who routinely collects cash-register or ATM receipts has probably noticed that they sometimes become unreadable in a matter of weeks. The ESI study of the Voter Verified Paper Audit Trail (VVPAT) records produced by the TS[X] machines in Cuyahoga County, Ohio showed a large fraction of them were unreadable. While Pennsylvania does not use VVPAT's, the same thermal printer is used to print the totals tape which Dr. Shamos appears to be suggesting could be used to comply with the permanent physical record requirement of the Pennsylvania Election Code.

---

[24] Obviously, there is no dispute that the printed vote records constitute a "physical record."

[25] While both parties agree that some of the DREs print vote records using other, more stable types of ink and paper, neither party has identified the specific machines that do so. Clearly, though, not all machines suffer from the alleged defect.

Petitioners' Ex. 7 at ¶ 36. While Petitioners acknowledge the opinion of the Secretary's expert, Dr. Shamos,[26] that, if thermal paper is kept away from direct exposure to heat, its legibility will exceed the federal twenty-two month ballot retention period, they argue that nothing in the record suggests that "busy election workers, without direction or even suggestion from the Secretary, are taking it upon themselves to store [cast vote records] in climate controlled containers." Petitioners' memorandum of law at 42.

Obviously, with respect to the electronic voting machines that do not print vote records on thermal paper, there is no issue as to the permanency of the paper records. As to the unspecified machines which allegedly use thermal paper, Dr. Jones' opinion regarding the permanency of thermal paper is too vague and non-specific to declare as a matter of law that vote records printed on thermal paper are not permanent. In addition, as we noted above, the possibility that vote records printed on thermal paper may not be treated properly to ensure their stability and longevity does not require a declaration that the machines cannot provide a permanent record.

---

[26] Dr. Shamos opined in his report that:

> [D]r. Jones declares, without citation, that "the same thermal printer is used to print the totals tape which Dr. Shamos appears to be suggesting could be used to comply with the permanent physical record requirement of the Pennsylvania Election Code." While that may be true of some of the printers used in Pennsylvania, it is not true of all of them, and Dr. Jones has not identified which ones he believes use thermal paper. It is true that thermal paper must be kept away from direct exposure to heat in order to remain readable. However, if this is done, thermal paper far exceeds the 22-minth [sic] ballot retention requirement. I personally possess thermal totals tapes from examinations that occurred more than 10 years ago that are still readable.

Respondent's Ex. 30 at ¶ 41(footnote omitted)

Next, while Petitioners do not dispute that the printed (paper) vote records satisfy the requirement for a "physical record," they contend that the electronic vote records do not.

> Although courts have struggled with the nature of electronic data in other contexts, ultimately the answer turns on what the General Assembly intended. In this context, the General Assembly cannot have intended electrons – subatomic particles so small that they cannot be observed with the naked eye – to satisfy the Election Code. *See, e.g.*, Jones Report ¶ 38 ("the electrons uses [sic] to record data . . . cannot be observed without the aid of complex technology such as an electron microscope or a computer.)"
>
> If the General Assembly truly intended that purely electronic data would be sufficient, it could have required that [electronic voting systems] provide for a "permanent electronic record."

Petitioners' memorandum of law at 36 (footnote omitted). Whether the General Assembly intended or considered vote records stored on electronic media to satisfy the requirement for a "permanent physical record," while an interesting question, is not one that needs to be resolved in light of the undisputed fact that every certified DRE at issue in this lawsuit can provide vote records printed on paper.

Finally, Petitioners contend that the electronic vote records, including the cast vote records or ballot images from which the printed records stem, cannot be deemed a "record of each vote cast" because there is no way to certify that the records accurately represent each vote cast. According to Petitioners, the vote records are "software dependent" and, therefore, are vulnerable to all the various undetectable maladies plaguing computers and computer software. Specifically, Petitioners argue:

> [E]ven if the data that is stored electronically on DREs were both "permanent" and "physical," there is no way

for the Secretary (or anyone else) to certify that it is a "record of each vote cast." Say what you will about paper ballots and the ability to alter them after they have been cast, the systems that incorporate paper ballots will always create an actual record of the actions as expressed by a voter. Even if they are altered after that, that does not change that there was at one time an actual, accurate record of the voter's actions.

The same cannot be said of DRE systems. . . . [E]ven the initial writing of data in a computer's memory is dependent on and affected by the software the computer runs, and if that software is flawed or corrupted, the initial data – and any subsequent copies of it – will not reflect the voter's interaction with the ballot interface. And as there was never a physical ballot to fall back on, the system in such a situation would never create any actual "record" of any actual vote. *See, e.g.*, Lopresti Report at 5 ("Since even the initial writing of a record into computer memory is accomplished through the use of software and hardware intermediaries, there is no way for a human observer to confirm that what is written is in fact an accurate record of his/her vote.") (Ex. 11); . . . [Jones] ¶ 42 (stating that voting data is "the product of complex computer software working from information retained from the time the voters cast their ballots" and discussing the "long chain of translation and copying that intervenes between the voter's act of casting a ballot and the creation of a permanent record of that act. We have no way of knowing, at each step along this chain of translation and copying, that the information conveyed correctly records each vote cast."). In short, whereas optical scan systems[27] use voter-created records, DREs generate software-created data that is no more reliable than the software itself. And when for whatever reason the software is not reliable, there is no "record" of the vote at all.

---

[27] With an optical scan voting system, the voter marks a paper ballot, which is then fed into an optical scanner to be read and tallied.

Petitioners' memorandum of law at 39-40 (footnote added). Petitioners' concerns, while understandable from a policy standpoint, do not entitle them to relief as a matter of law.

First, the Election Code was amended in 1980 to authorize the use of electronic voting systems. Electronic voting systems, as designed and defined, register votes electronically, without the need for use of paper ballots or "voter-created" records.[28] *A fortiori*, without software, we would not have electronic voting systems; software is necessary to register, create and store the voter's action in electronic format. Not only does the Code not require that vote records be software independent, but such a construction would be absurd, completely incongruous to the amendments defining and authorizing the use of such devices and inconsistent with the state of technology in 1980.[29] Second, while Petitioners

---

[28] *See* Section 1101-A (defining "voting device" to include an apparatus by which *votes are registered electronically*). *See also* Section 1118-A, added by the Act of July 11, 1980, P.L. 600, 25 P.S. § 3031.18 (pertaining to recounts and differentiating between electronic voting systems that utilize paper ballots and those that do not).

[29] When the Election Code was amended in 1980 to authorize the use of electronic voting systems, computer equipment and programs were not only an established and accepted technology and business commodity, but were beginning to be marketed to consumers for personal use. *See generally Computer Print Systems, Inc. v. Lewis*, 422 A.2d 148 (Pa. Super. 1980) (addressing, *inter alia*, whether computer programs were type of property which would qualify as trade secrets); *In re Data General Corp. Antitrust Litigation*, 490 F. Supp. 1089 (N.D. Ca. 1980) (addressing, *inter alia*, claim that Data General tied licensing of its software to sale of its central processing units in violation of federal antitrust laws); History of Computers at http://homepage.cs.uri.edu/faculty/wolfe/book/Readings/Reading03.htm; Computer History Museum-Timeline of Computer History at http://www.computerhistory.org/timeline/?category=cmptr. *See also* Legislative Journal-House, No. 55 of 1980 (July 2, 1980) at 2041, Petitioners' Exhibit 46 (Rep. Taddonio stating that: "Right now there are a lot of advances being made [in the computer industry]. We read in the papers that Radio Shack has computers for $500. . . . It will not be long until it becomes economically feasible to have individual computers at the field site where we can have counting at the precinct level and decentralize the election . . . .").

are obviously concerned with the vulnerability of the DREs to "malicious or mistaken code, or . . . [a highjack] through a 'man-in-the-middle' attack, or [human error],"[30] the certification and approval process is designed to provide security from such occurrences.[31] In addition, according to Dr. Shamos:

> [I]t is possible to determine easily whether a system is recording, computing and tabulating votes accurately. One casts a known set of ballots that have been previously tabulated manually. A totals report is then produced and the machine totals are compared with those reported by the machine. This is done on a large scale by the [Independent Test Authority] and on a small scale during certification exams.

Petitioners' Ex. 2, Shamos Report at ¶ 259 (responding to interrogatories). Dr. Shamos also noted that machines are tested before each election to verify that they are recognizing votes correctly. *Id.* at ¶ 423. Accordingly, we deny Petitioners' motion for summary judgment as to Count I.

Next, Petitioners contend that they are entitled to summary judgment with respect to Count IV because the DREs do not permit a statistical recount using a device of a type different than that used for the specific election as required by Section 1117-A. Section 1117-A provides:

---

[30] Petitioners' Reply at 8.

[31] *See* Section 1107-A, 25 P.S. § 3031.7 (pertaining to requirements of electronic voting systems). *See also* Petitioners' Ex. 2, Shamos Report at ¶ 64 (discussing ITA [Independent Test Authority] testing and Secretary's certification and noting in pertinent part: "[A] review is made to determine whether there are security vulnerabilities that could feasibly be exploited by a person who gains access to the system during the election process, and a check is made to determine the degree to which the system resists attempts to alter its records."); and at ¶ 246 (noting that federal testing includes, *inter alia*, "system security"). Dr. Shamos also opined that electronic records use mechanisms that protect from and detect alterations." *Id.* at ¶¶ 113, 116. Obviously, human error cannot be addressed with design specifications but can be minimized with proper and thorough training.

> The county board of elections, as part of the computation and canvass[32] of returns, shall conduct a statistical recount of a random sample of ballots after each election using manual, mechanical or electronic devices of a type different than those used for the specific election. The sample shall include at least two (2) per centum of the votes cast or two thousand (2,000) votes whichever is lesser [footnote added].

There is no dispute that the certified DREs can provide printed copies of the electronically recorded vote records (ballot images) and that these records can be counted manually. Nor does there appear to be any dispute that the removable electronic media containing the vote records can be removed and inserted into a different type of machine, read and tabulated separately. *See generally* Respondent's Ex. 9, Shamos Report at ¶¶ 120, 169; Petitioners' Ex. 7, Jones Report at ¶¶ 58-63. Petitioners contend, however, that these alternate means of conducting a recount fail to satisfy Section 1117-A because the same hardware and software used to create and save/store the vote records is used to retrieve the saved data and print it out for manual counting. According to Petitioners, "it is impossible to generate any record of election results, electronic or paper, without using the same software that collected the data and wrote it to memory in the first instance." Petitioners' memorandum of law at 55. In Petitioners' view, the lack of a software-independent vote record precludes a recount by a device of a different

---

[32] Section 102 of the Election Code defines "canvass" to "include[ ] gathering the ballots after the election and counting, computing and tallying the votes." 25 P.S. § 2601. For purposes of Article XI-A of the Code (Electronic Voting Systems), "ballot" is defined to mean: "ballot cards or paper ballots upon which a voter registers or records his vote *or the apparatus by which the voter registers his vote electronically* and shall include any ballot envelope, paper or other material on which a vote is recorded for persons whose names do not appear on the ballot labels." 25 P.S. § 3031.1 (emphasis added). Although not relevant here, "ballot card," "ballot label" and "paper ballot" are all statutorily defined.

type. According to Petitioners, only voting systems employing a physical ballot, such as punch-card ballots, which are read by a card reader, and voter-marked paper ballots, which are optically scanned, satisfy this provision. We disagree.

First, as already noted, the Election Code does not require software-independent vote records. *See* Section 1107-A (mandatory specifications established for electronic voting systems; production of software-independent vote records not included). Indeed, in addition to authorizing voting devices employing ballot cards and punch cards, the Code specifically authorizes systems which only register votes electronically. *See* Section 1101-A (defining "voting device"); Section 1404(e)(4), 25 P.S. § 3154(e)(4) (pertaining to recount or recanvass of votes in districts using electronic voting systems); Section 1702, 25 P.S. § 3262 (pertaining to recanvassing voting machines, including electronic voting systems that do not utilize paper ballots).

Second, as noted by the Secretary, Section 1117-A provides only that the statistical sample of ballots must be *counted* using a different method or device; there is no requirement that the ballots included in the recount must be produced using a separate device. Thus, the DREs, capable of producing vote records which can be manually counted, satisfy the requirements of Section 1117-A.

In reaching this conclusion, we reject Petitioners' contention that one of the purposes of Section 1117-A is to verify whether the EVS correctly captured voter intent.[33] Petitioners maintain:

---

[33] According to Petitioners, Section 1117-A requires more than a simple retally of votes. Rather, looking to other recount provisions of the Election Code, specifically Section 1701, 25 P.S. § 3261 (pertaining to the opening of ballot boxes upon petition), Petitioners contend that the General Assembly intended Section 1117-A to serve as an audit. Petitioners believe that unlike punch card and optical scan systems, which generate a permanent physical record of each vote **(Footnote continued on next page...)**

> [I]n order to perform this mandatory verification, it is necessary to have captured the voter's intention, that is, the record of the voter's choices on the original ballot, separately and distinctly from the software that wrote the selections onto electronic memory and then counted the electronic memory. [Here, with the certified DREs,] the county elections board has no record of the voter's intent, it is impossible to verify whether the DRE captured it correctly, and therefore impossible to determine whether the computer counted correctly.

Petitioners' memorandum of law at 52 (footnote omitted).

We agree with the Secretary that Section 1117-A contemplates nothing more than a recount or retally of a specified number of ballots recorded during an election. Inasmuch as the Code clearly authorizes voting systems that record votes electronically without use of a physical ballot, and that the recount

---

(continued...)

cast that can later be compared with the election results, the DREs do not provide a "record of the voter's intent, [so] it is impossible to verify whether the DRE captured it correctly, and therefore impossible to determine whether the computer counted correctly." Petitioners' memorandum at 52 (footnote omitted).

Section 1701 is simply not applicable. That section provides, *inter alia*, that upon petition of electors alleging that they believe fraud or error was committed in the computation of votes, marking of ballots or otherwise in connection with such ballots, the court shall *open the ballot box* and cause the entire vote of the election district to be correctly counted. Section 1701 applies, however, only if the election district uses electronic voting systems utilizing paper ballots. *See* Section 1118-A(1), added by the Act of July 11, 1980, P.L. 600, 25 P.S. § 3031.18(1). If a recount is ordered in a district that uses any other type of EVS, the recount shall by conducted under Section 1702, 25 P.S. § 3262 (pertaining to recanvassing voting machines upon petition). Section 1702 provides for the recount of all votes cast on a voting machine(s). Unlike Section 1701, however, Section 1702 makes no mention of opening the ballot box or error or fraud in connection with marking of ballots because obviously, paper ballots were not used. Rather, Section 1702 provides that the court shall make visible the registering counters of the voting machine(s) and "recanvass the vote cast therein" based upon a petition alleging fraud or error in the canvassing of votes cast. Since Section 1702 applies when the voting machine does not utilize any type of ballot card, verification of voter-intent via a comparison of recorded electronic data with some other indicia of voter intent is neither contemplated nor provided for.

provision applicable to such systems when an allegation of fraud or error is made does not require comparison of electronic records with physical records demonstrating voter intent, Section 1117-A, which requires only an automatic recount of a statistical sample, cannot be construed as Petitioners suggest.[34]

Finally, Petitioners have requested summary judgment with respect to Count VI, pertaining to the reexamination of previously certified electronic voting systems pursuant to Section 1105-A, 24 P.S. § 3031.5. Pursuant to Section 1105-A(a), the Secretary is required to reexamine such voting systems upon proper request by ten or more qualified registered electors who have paid the requisite fee. Essentially, Petitioners ask this Court to issue a writ of mandamus against the Secretary, directing her to conduct the requested reexaminations.[35] There is no dispute that valid requests for reexamination were made and that they were initially denied by the prior Secretary. The Secretary's duty to re-examine the machines upon proper request is mandatory.

The Secretary contends, however, that this matter is now moot, averring in her brief: "On July, 25, 2011, the Secretary . . . acknowledged that her office had a duty under section 3031.5 and, therefore, determined that a re-

---

[34] Petitioners have also requested judgment in their favor with respect to Counts IX and X on the ground that the Secretary's allegedly improper certification of the DREs at issue resulted in constitutional violations as well. Because we have concluded that Petitioners have not demonstrated that the certifications were illegal thereby entitling them to judgment as a matter of law, we also deny Petitioners' motion for judgment regarding Counts IX and X.

[35] "It is settled beyond question ... that mandamus, an extraordinary writ, is not granted as a matter of right but as a matter within the sound discretion of the court...." *Bobick v. Fitzgerald*, 416 Pa. 588, 591-92, 207 A.2d 878, 880 (1965) (citations and quotation marks omitted). Moreover, "so drastic a procedure can, and only should, be permitted when the complaining person has a clear, legal right . . . and the defendant has a clear, legal duty *which he has refused to perform*." *Zaccagnini v. Borough of Vandergrift*, 395 Pa. 285, 289, 150 A.2d 538, 540 (1959) (emphasis added).

examination of the three DREs would be appropriate. . . . The Secretary directed her staff to arrange those re-examinations, which will likely be completed before the 2012 primary elections." Respondent's brief at 66 (citing to Respondent's Ex. 4).

We disagree that the matter is moot because it is not clear whether the examinations have been completed. However, because the Secretary has agreed to conduct the reexaminations and the process has clearly started, we decline to issue a writ of mandamus against the Secretary of the Commonwealth at this time. Rather, we direct the parties to file a status report regarding whether the requested reexaminations have been completed within 15 days of the filing date of our opinion and order.

Based upon the foregoing, Petitioners' motion for partial summary judgment is denied.

BONNIE BRIGANCE LEADBETTER,
President Judge

Judge Brobson did not participate in the decision in this case.

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	No. 442 M.D. 2006
	:	Argued: November 16, 2011
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

ORDER

AND NOW, this 29th day of August, 2012, Petitioners' Motion for Partial Summary Judgment is denied. Furthermore, in accordance with the foregoing opinion, the parties shall file a status report with the Court within 15 days of this Order.

BONNIE BRIGANCE LEADBETTER,
President Judge

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
	:	No. 442 M.D. 2006
v.	:	
	:	Argued: November 16, 2011
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

BEFORE: HONORABLE BONNIE BRIGANCE LEADBETTER, President Judge
HONORABLE BERNARD L. McGINLEY, Judge
HONORABLE DAN PELLEGRINI, Judge
HONORABLE RENÉE COHN JUBELIRER, Judge
HONORABLE ROBERT SIMPSON, Judge
HONORABLE MARY HANNAH LEAVITT, Judge
HONORABLE PATRICIA A. McCULLOUGH, Judge

CONCURRING AND DISSENTING
OPINION BY JUDGE McCULLOUGH FILED: August 29, 2012

I concur with the Majority's disposition of Counts IV, VI, IX, and X. However, I would grant Petitioners' motion for summary judgment on Count I

because the Direct Recording Electronic Voting Systems (DREs) fail to "provide for a permanent physical record of each vote cast."

Section 1101-A of the Pennsylvania Election Code (Code),[1] defines "Electronic voting system" as:

> a system in which one or more voting devices are used to permit the registering or recording of votes and in which such votes are computed and tabulated by automatic tabulating equipment. The system shall provide for a permanent physical record of each vote cast.

(Emphasis added.)

Petitioners' motion for summary judgment on Count I avers that there is no genuine issue of material fact that DREs fail to, "provide for a permanent physical record of each vote cast." In my view, based on the record and clear statutory language, the electronic data stored in DREs is neither "permanent," nor "physical."

The experts' analysis of the electronic data itself would render the data stored electronically on DREs as not "permanent" and subject to intentional and unintentional alteration which can occur in ways that are undetectable. Making "print-outs" of each vote does not constitute a "permanent physical record." Respondent's expert testified at his deposition that vote receipts could be printed out on receipt-grade, ribbon-like thermal paper but acknowledged that thermal paper can become unreadable in a matter of weeks. Such paper is simply

[1] Act of June 3, 1937, P.L. 1333, as amended, added by the Act of July 11, 1980, P.L. 600, 25 P.S. §3031.1.

not "permanent." See Lopresti Report at 4-5 (Ex. 11); see also Jones Report ¶ 30-32 (Ex. 7).[2]

In addition to not being permanent, the data stored electronically on DREs is not physical. If the General Assembly intended electronic data to be considered "physical," section 1101-A of the Code would have required DREs to provide for a "permanent electronic record" (emphasis added) rather than a "permanent physical record." While a memory card or computer chip containing electronic data is "physical," it is not the "record of each vote cast," which is the clear language of the statute.

Accordingly, I would grant Petitioners' motion for summary judgment on Count I.

PATRICIA A. McCULLOUGH, Judge

Judge Pellegrini joins.

---

[2] As Dr. Lopresti explained, electronic data cannot be considered "permanent" because by its very nature it is subject to alteration and change:

> Computer memory can be written or rewritten with incorrect data intentionally (as a result of software and/or hardware and/or human error) or unintentionally (as a result of a malicious attempt to alter the results of an election). Moreover, the act of writing computer memory is in principle undetectable; it leaves behind no physical evidence.... Since even the initial writing of a record into computer memory is accomplished through the use of software and hardware intermediaries, there is no way for a human observer to confirm that what is written is in fact an accurate record of his/her vote.

Lopresti Report at 4-5 (Ex. 11); see also Jones Report ¶ 30-32 (Ex. 7).

EXHIBIT B

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	No. 442 M.D. 2006
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

ORDER

AND NOW, this 29th day of January, 2013, it is hereby ORDERED that:

1. Count VI of the above-captioned Petition for Review is DISMISSED as moot.

2. For the reasons stated in this Court's decision of August 29, 2012, Counts I, IV, and V are DISMISSED.

3. Election Systems & Software, Inc. may file a supplement to its Response to the Petitioners' outstanding Motion to Compel (filed July 28, 2011) within 7 days (i.e., February 5, 2013);

4. Hart InterCivic, Inc. may file a response to the above referenced Motion to Compel within 7 days (i.e., February 5, 2013);

5. Petitioners may supplement their discovery requests within 7 days;

6. Discovery shall be closed as of March 7, 2013;

7. Within 14 days following the close of discovery, the Secretary may supplement her Motion for Summary Relief on the remaining counts; Petitioners may file a response within 14 days.

Further, if following the Court's ruling on Respondent's Motion for Summary Relief, issues of fact remain to be tried, trial shall be scheduled by further order of the Court.

Bonnie B. Leadbetter

BONNIE BRIGANCE LEADBETTER,
Judge

EXHIBIT C

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	No. 442 M.D. 2006
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

BEFORE: **HONORABLE BONNIE BRIGANCE LEADBETTER,** Judge

OPINION NOT REPORTED

MEMORANDUM OPINION BY JUDGE LEADBETTER **FILED: October 1, 2013**

The Secretary of the Commonwealth (Secretary) seeks summary relief on the six counts (out of ten) remaining undecided in the action by twenty-four individual voters,[1] who seek an order in mandamus directing the Secretary to de-

[1] Specifically, Petitioners are Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs–Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary **(Footnote continued on next page...)**

certify specific electronic voting systems (DREs) currently used in some counties in the Commonwealth.[2] For the reasons that follow, the motion is granted.

This is the fourth time this case is before the court. Previously, we denied the Secretary's preliminary objections to the petition for review. *See Banfield v. Cortes (Banfield I)*, 922 A.2d 36 (Pa. Cmwlth. 2007) (en banc), permission to appeal denied by Supreme Court order dated December 16, 2008 (70 MM 2007). Thereafter, we also denied the Petitioners' motion for partial summary judgment on Counts I (DREs fail to provide a permanent physical record), IV (DREs fail to provide for a recount as required under the Pennsylvania Election Code[3]), VI (Secretary failed to perform a required reexamination of the DREs), IX (certification process violates the equal protection clause, Article I, § 26 of the Pennsylvania Constitution), and X (certification process violates the uniformity requirement in Article VII, § 6 of the Pennsylvania Constitution). *See Banfield v. Aichele (Banfield II)*, 51 A.3d 300 (Pa. Cmwlth. 2012) (en banc). Subsequently, based on the rationale underpinning the rulings in *Banfield II*, the court dismissed Counts I, IV, V, VI and, dismissed as moot Count VI inasmuch as the Secretary performed the reexamination sought therein. *See Banfield v. Aichele*, No. 442 M.D. 2006, Order filed January 29, 2013. Presently, the Secretary seeks summary relief on Count II (DREs susceptible to fraud), Count III (certification procedures

---

(continued...)

Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero and Jeanne Zang.

[2] The voting machines subject to this challenge are: the ELECTronic 1242, made by Danaher Industrial Controls; the AccuVote TSX, made by Diebold Election Systems, Inc. (now Dominion); the iVotronic, made by Elections Systems & Software, Inc.; the eSlate, made by Hart InterCivic, Inc.; the AVC Edge II and the AVC Advantage, made by Sequoia Voting Systems, Inc. (now Dominion).

[3] Act of June 3, 1937, P.L. 1333, *as amended*, 25 P.S. §§ 2600-3591.

inadequate), Count VII (testing procedures inadequate), Count VIII (likely failure to count all votes accurately in violation of Article I, § 5 of the Pennsylvania Constitution concerning free and equal elections), Counts IX and X (equal protection and uniformity violations of state constitution).[4]

In Counts II, III and VII, Petitioners seek relief based on failure to comply with certain requirements imposed under Section 1107-A of the Election Code, added by the Act of July 11, 1980, P.L. 600, 25 P.S. § 3031.7. The pertinent provisions of Section 1107-A direct:

> No electronic voting system shall, upon examination or reexamination, be approved by the Secretary of the Commonwealth, or by any examiner appointed by him, unless it shall be established that such system, at the time of such examination or reexamination:
>
> . . . .
>
> (11) Is suitably designed for the purpose used, is constructed in a neat and workmanlike manner of durable material of good quality, is safely and efficiently useable

---

[4] Summary relief in the form of a judgment in favor of the Secretary may be granted only in those cases "where the record clearly shows that there are no genuine issues of material fact and that the moving party is entitled to judgment as a matter of law." *P.J.S. v. Pa. State Ethics Comm'n*, 555 Pa. 149, 153, 723 A.2d 174, 176 (1999). Moreover, "[w]hen resolving a motion for summary judgment, the record must be viewed in the light most favorable to the opposing party, and all doubts as to the existence of a genuine issue of material fact must be resolved in favor of the nonmoving party." *Id.*

Pursuant to Pa. R.A.P. 1532 this court may, upon application, enter summary relief "at any time after the filing of a petition for review" if the right of the applicant is clear. In the present case, the court ordered discovery to be completed by March 7, 2013. *See* Order dated January 29, 2013. Nonetheless, Petitioners have filed a motion to compel production of documents containing over 642 communications that Respondents redacted or withheld, which remains pending. See Motion to Compel the Production of Documents filed March 15, 2013. Having reviewed these documents in camera, it is apparent that the additional documents and information sought by Petitioners will not yield evidence that the machines fail to comply with the statutory requirements for accuracy and security.

> in the conduct of elections and, with respect to the counting of ballots cast at each district, is suitably designed and equipped to be capable of absolute accuracy, which accuracy shall be demonstrated to the Secretary of the Commonwealth.
>
> (12) Provides acceptable ballot security procedures and impoundment of ballots to prevent tampering with or substitution of any ballots or ballot cards.
>
> (13) When properly operated, records correctly and computes and tabulates accurately every valid vote registered.
>
> . . . .
>
> (16) If the voting system is of a type which provides for the computation and tabulation of votes at the district level, the district component of the automatic tabulating equipment shall include the following mechanisms or capabilities:
>
> . . . .
>
> (iii) It shall be so constructed and controlled that, during the progress of voting, it shall preclude every person from . . . tampering with the tabulating element.
>
> . . . .

25 P.S. § 3031.7 (11) -(13), (16)(iii). In addition, subsection (17)(i) of 1107-A, 25 P.S. § 3031.7(17)(i), imposes the same tamper-proof requirement to systems that compute and tabulate votes at a central counting center. Essentially, Petitioners aver that the challenged DREs are not capable of the required accuracy and are not sufficiently tamper-proof, that the Secretary's testing procedures fail to ensure full compliance with all of the statutory requirements listed above and that the Secretary has failed in her duty to adopt adequate testing procedures.

In general, mandamus is available only to a plaintiff who establishes a clear legal right to compel the official performance of a ministerial act or mandatory duty and there is no other adequate remedy at law. *Banfield I*, 922 A.2d

at 42. In the present case, where mandamus is not sought based on the Secretary's failure to certify DREs as required under the Election Code but on the premise that she failed to properly exercise her discretion in the performance of this duty, Petitioners must establish that the Secretary performed her statutory duties arbitrarily, fraudulently or under a mistake of law. *Id.* The standard for affording mandamus relief does not encompass a review of the Secretary's discretion in how she performed her duties so as to impose the court's view as to how these duties should be performed. *Maxwell v. Bd. of Dirs. Sch. Dist. of Farrell*, 381 Pa. 561, 566, 112 A.2d 192, 195 (1955): *Chadwick v. Dauphin County Office of the Coroner*, 905 A.2d 600, 604 (Pa. Cmwlth. 2006). To a large degree, this inappropriate oversight is exactly what Petitioners seek.

In their brief, Petitioners characterize their cause of action as "a case about how closely the court will monitor the executive's performance of its duty - entrusted to it by the legislature - to ensure the integrity of elections." Petitioners' Brief in Opposition to Summary Relief at 23. While this court has recognized its responsibility to protect the Commonwealth's interest in the integrity of the election process, *In re Carlson,* 430 A.2d 1210, 1212 (Pa. Cmwlth. 1981), that does not mean that courts have broad authority to prescribe the best way for the Secretary to perform her duties. *See Banfield I,* 922 A.2d at 44 (domain of the judiciary is to interpret, construe and apply the law). In order to prevail in their quest to de-certify the challenged DREs, Petitioners must establish that the DRE voting systems actually fall short of the statutory requirements for accuracy and security from tampering. *See Davidowitz v. Philadelphia County*, 324 Pa. 17, 187 A. 585 (1936) (in a challenge to use of "voting machines" the court refused to enjoin their use absent a clear legislative or constitutional violation). To survive

the present motion for summary judgment in favor of the Secretary, the record must contain some evidence that would support such a finding. *See Young v. Dep't of Transp.*, 560 Pa. 373, 376, 744 A.2d 1276, 1277 (2000). In this case, where the subject of inquiry, i.e., the workings of electronic voting systems, is outside the skill and knowledge of the ordinary layman, Petitioners cannot prevail in their cause of action without supportive expert opinion. *Id.* at 376, 744 A.2d at 1278. Petitioners have come forward with no evidence that the challenged machines fail to accurately record votes when properly used. Rather, review of the expert reports discloses that Petitioners can establish no more than that a possibility exists that the challenged DREs could in theory be subject to tampering or human error. But in this regard the challenged systems do not differ from any other voting system.

On behalf of Petitioners, Dr. Daniel Lopresti, a Professor and Chair of the Department of Computer Science and Engineering at Lehigh University, opined that the Secretary's certification process was inadequate in that it failed to give sufficient attention to security vulnerabilities identified in three studies that are well known in the field. Specifically, Lopresti points to the program tampering accomplished during a laboratory challenge conducted at Princeton University, known as the "Hursti exploit," the detailed source code and penetration testing that revealed security vulnerabilities in California's "Top to Bottom Review," and similar vulnerabilities demonstrated in Ohio's "EVEREST study." Petitioners' Exh. 18 in Opposition to Summary Relief, Lopresti Report at 6-8. These studies demonstrate vulnerabilities, worthy perhaps of consideration in the evolution of technological improvements, but the possibility that tampering can produce inaccuracy does not render the DREs incapable of the absolute accuracy required under the Election Code. Capability and vulnerability are not mutually exclusive

characteristics, i.e., capable of accuracy does not mean invulnerable to tampering. Furthermore, the fact that these studies uncovered vulnerability does not establish the presence of unacceptable security procedures. Testing machine vulnerabilities does not fully test security procedures that encompass not only tamper-proofing built into the electronics but also measures to check and cross-check human activity in the conduct of elections.

Similarly, Petitioners' expert, Dr. Douglas W. Jones, a Professor at the University of Iowa, opined that the challenged DREs' software is a "systematic source of security vulnerabilities" rendering the DREs not suitably designed for the purpose used and not constructed in a workmanlike manner. Petitioners' Exh. 22 in Opposition to Summary Relief, Jones Report at ¶¶ 29 – 40. Jones's expert report, while noting specific vulnerabilities identified in the California and Ohio studies, does not conclude that the machines are incapable of doing what they are designed to do – count and tabulate votes. Vulnerability to tampering or manipulation exists now and has existed since voting began. In his report, Jones recognized that:

> Secure voting is very difficult, whether done using manual, mechanical or electronic means. While the algorithms involved are trivial, requiring nothing more than a sum, for each candidate or ballot position, of the number of votes, the distributed nature of the computation and the number of participants pose immense problems. Elections involve an appreciable fraction of the entire national population as participants, and the history of election fraud includes examples that were perpetrated by every class of participant, from voter to polling place election judge to election administrator to voting system maintenance technician.

Jones Report at ¶ 18. Indeed, even paper ballots can be destroyed or altered if those with access to the voting and tabulation process are intent on fraudulent manipulation of results, perhaps even more easily than electronic machines since

no technical expertise is required. Since voting will always be vulnerable to fraud, a mere possibility of a security breach is not alone sufficient to warrant overriding the Secretary's determination to certify the systems. While the expert reports call attention to perceived problems, they do not establish that the machines used successfully for many elections are necessarily fatally flawed.

Furthermore, the identification of certain vulnerabilities discovered in tests conducted in California or Ohio does not establish that the Secretary's testing was fatally defective. There is not a dispute here as to whether the DREs are imperfect; the challenged DREs, as well as the electronic voting systems the Petitioners point to as preferable, are imperfect. There is also no dispute that testing procedures are not, and cannot be, perfect. However, the present cause of action fails nonetheless because the experts have failed to establish that the Secretary's testing procedures and the DREs that she certified create more than a mere possibility of error in recording and tabulating votes. If the mere possibility of such error were considered sufficient to bar use of a voting system then we would be left with none.

Courts confronted with similar challenges based on the possibility of vote miscount have reached similar conclusions. As the court in *Weber v. Shelley*, 347 F.3d 1101 (9th Cir. 2003), observed:

> No balloting system is perfect. Traditional paper ballots, as became evident during the 2000 presidential election, are prone to over-votes, under-votes, hanging chads, and other mechanical and human errors that may thwart voter intent. . . . The unfortunate reality is that the possibility of electoral fraud can never be *completely* eliminated, no matter which type of ballot is used.

Id. at 1106 – 7 (emphasis in original). In *Wexler v. Anderson*, 452 F.3d 1226 (11th Cir. 2006), the court indicated that *likelihood or probability* of vote miscount, *not*

its mere possibility, is required to trigger strict scrutiny of state recount procedures, stating that:

> Plaintiffs' fundamental error is one of perspective. By adopting the perspective of the residual voter [i.e., a voter who upon a recount will have his paper or optical scan ballot examined manually for voter intent], they avoided the question that is of constitutional dimension: Are voters in touchscreen counties less likely to cast an effective vote than voters in optical scan counties?
>
> . . . .
>
> [I]f voters in touchscreen counties are burdened at all, that burden is the mere possibility that should they cast residual ballots, those ballots will receive a different, and allegedly inferior, type of review in the event of a manual recount.

Id. at 1231-32. In *Hennings v. Grafton*, 523 F.2d 861 (7th Cir. 1975), the court opined that, "[T]he failure of election officials to take statutorily prescribed steps to diminish what was at most a theoretical possibility that devices might be tampered with . . . fall[s] far short of constitutional infractions." *Id.* at 864. This court is firmly persuaded that more than a mere possibility of inaccuracy or insecurity is required to justify the relief Petitioners seek.

Further, Counts VIII,[5] IX[6] and X[7] allege that the inadequate testing and improper certification of the DREs allows for the use of systems that fail to

---

[5] Count VIII alleges that certification of the challenged DREs "create the risk that persons for whom the majority of voters have not cast their ballots will be declared the election winners and will take office, in contravention of the very essence of our democracy." Petition for Review at 32, ¶ 134. Petitioners maintain that this transgresses the guaranty in Article I, § 5 of the Pennsylvania Constitution that: "Elections shall be free and equal; and no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage."

[6] Count IX alleges that certification of the challenged DREs "threatens Petitioners' fundamental right to vote because the voting systems' defects and security flaws create the risk that Petitioners, together with other Pennsylvania voters, have their votes rendered meaningless or, worse yet, deemed cast for a candidate for whom they did not vote." Petition for Review at 33, ¶ 138. Petitioners assert that this interference with the right to vote violates the guaranty in

(Footnote continued on next page...)

ensure that votes will be honestly captured and counted as cast, thus interfering with the Petitioners' fundamental right to vote and discriminating against those forced to use the challenged DREs. Petitioners' Brief in Opposition to Summary Relief at 47. These constitutional challenges, based as they are on the premise that the challenged DREs are so inaccurate and insecure as to infringe on the right to vote and the requirement for uniform election regulation, cannot survive inasmuch as Petitioners are unable to prove their starting premise.

Accordingly, the Secretary's application for summary relief is granted.

Bonnie B. Leadbetter

BONNIE BRIGANCE LEADBETTER,
Judge

(continued...)

Article I, § 26 of the Pennsylvania Constitution that: "Neither the Commonwealth nor any political subdivision thereof shall deny to any person the enjoyment of any civil right, nor discriminate against any person in the exercise of any civil right."

[7] Count X alleges that: "Because the likelihood of an inaccurate tally that cannot be audited is greater in counties using the certified DRE voting systems than in counties that use systems that permit independent recounts upon an allegation of error or fraud, the use of the certified DRE voting systems threatens to create an imbalance in the weight given to the votes in the various counties, thereby depriving all Pennsylvania citizens, including Petitioners of the uniformity rights and equal protection rights secured under the Pennsylvania Constitution." Petition for Review at 35, ¶ 144. Petitioners assert that this violates the prescription in Article VII, § 6 that: "All laws regulating the holding of elections by the citizens . . . shall be uniform throughout the state."

EXHIBIT D

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	No. 442 M.D. 2006
Carol Aichele, Secretary of the Commonwealth, Respondent	:	

ORDER

AND NOW, this 1st day of October, 2013, Respondent's Application for Summary Relief is granted. Judgment in favor of the Respondent shall be entered on Counts II, III, VII, VIII, IX and X of the Petition for Review.

Bonnie B. Leadbetter

BONNIE BRIGANCE LEADBETTER,
Judge

EXHIBIT E

IN THE COMMONWEALTH COURT OF PENNSYLVANIA

Mark Banfield, Sarah Beck, Joan Bergquist, Alan Brau, Lucia Dailey, Peter Deutsch, Constance Fewlass, Barbara Glassman, Marijo Highland, Janis Hobbs-Pellechio, Deborah Johnson, Andrew McDowell, James Michaels, J. Whyatt Mondesire, Mary Montresor, Rev. James Moore, Cathy Reed, Regina Schlitz, Alexander Sickert, Daniel Sleator, Susanna Staas, Stephen J. Strahs, Mary Vollero, Jeanne Zang, Petitioners	:	
v.	:	
Carol Aichele, Secretary of the Commonwealth, Respondent	:	No. 442 M.D. 2006

NOTICE OF JUDGMENT

Now, October 15, 2013, judgment in favor of respondent and against petitioners is hereby entered on Counts I, II, III, IV, V, VI, VII, VIII, IX, and X of the petition for review pursuant to a praecipe filed by counsel for petitioners.

Michael F. Krimmel,
Chief Clerk

Certified from the Record

OCT 16 2013

And Order Exit