IN THE COMMONWEALTH COURT OF PENNSYLVANIA

NO. 442 M.D. 2006

MARK BANFIELD, et al.,

Petitioner,

v.

CAROL AICHELE,
Secretary of the Commonwealth,

Respondent.

Petition for Review in the Nature of
an Action for Mandamus and in Equity

PETITIONERS' OPPOSITION TO RESPONDENT'S APPLICATION FOR SUMMARY RELIEF

Michael P. Daly
(PA Id. No. 86103)
Meredith N. Reinhardt
(PA Id. No. 93504)
Katie L. Bailey
(PA Id. No. 308748)
Drinker Biddle & Reath LLP
One Logan Square, Suite 2000
Philadelphia, PA 19103-6996
Phone: 215.988.2700
Fax: 215.988.2757

Michael Churchill
(PA Id. No. 4661)
Benjamin D. Geffen
(PA Id. No. 310134)
Public Interest Law Center
of Philadelphia
United Way Building, 2nd Floor
1709 Benjamin Franklin Parkway
Philadelphia, PA 19103
Phone: 215.627.7100
Fax: 215.627.3183

Marian K. Schneider
(PA Id. No. 50337)
Attorney-at-Law
295 E. Swedesford Road #348
Wayne, PA 19087
Phone: 610.644.1255
Fax: 610.644.1277

Counsel for Petitioners

Date: April 11, 2013

TABLE OF CONTENTS

TABLE OF CONTENTS

TABLE OF AUTHORITIES iv

I. INTRODUCTION 1

II. STANDARD AND SCOPE OF REVIEW 2

A. Standard of Review 2

B. Scope of Review 3

III. BACKGROUND 4

A. The General Assembly Repeatedly Rejects Bills That Would Have Allowed EVSs But Not Required That They Create Recountable Records and Preclude Tampering 4

B. The General Assembly's Concerns About The Security and Reliability of EVSs Were Shared By Scientists Who Were Familiar With Electronic Voting 7

C. Respondent Certifies DREs For Use In Commonwealth Elections Despite Having Conducted No Meaningful Security Tests Of Her Own 8

D. Respondent Refuses To Reexamine DREs Despite A Growing Consensus That They Do Not Prevent Every Person From Tampering With Them 10

1. 2005 Report of the Brennan Center Task Force on Voting System Security 10

2. 2006 Princeton Report on Security Analysis of the Diebold AccuVote-TS 11

3. 2007 Report of Florida State University Information Technology Laboratory 12

4. 2007 California Top to Bottom Report 13

5. The 2007 Ohio EVEREST Report 14

6. 2011 Report of the Argonne National Laboratory 15

7. Petitioners' Expert Reports and Expert Testimony In This Proceeding....16
E. Respondent Eventually Reexamines DREs But Still Fails To Test Whether DREs Preclude Tampering With Ballots or Tabulating Elements....17

IV. ARGUMENT....18

A. Respondent's Legal Arguments Find No Support In The Law....18

1. Respondent Is Not Immune From Petitioners' Suit, Which Simply Seeks to Compel Her to Carry Out Her Duties Pursuant to the Election Code....18

2. Compelling Officials To Comply With The Election Code Does Not Trigger, Let Alone Offend, The Separation of Powers Doctrine....19

3. The Court Can Grant All of the Relief Requested in the Petition, Including A Writ of Mandamus Compelling Compliance with the Election Code....20

4. Respondent's Statutory Interpretations Are Not Entitled To Deference Because They Conflict With the Statute's Language and Legislative History....24

B. Respondent's Factual Arguments Find No Support In The Facts....27

1. There Is A Genuine Issue Concerning Whether DREs "Preclude" "Every Person" From Tampering with "Tabulating Elements"(Count II)....27

a. Whether DRE Tabulation Element Tampering Has In Fact Occurred In Pennsylvania Or Elsewhere Is Not A Material Fact....27

b. There Is A Genuine Issue Regarding Whether DREs "Preclude" "Every Person" From Tampering With The "Tabulating Element"....30

2. There Is A Genuine Issue Concerning Whether DREs Have "Acceptable Ballot Security" To "Prevent Tampering" With "Ballots" (Count II)....34

3. There Is A Genuine Issue of Material Fact Concerning Whether Respondent Uses Testing Procedures That Ensure DREs Comply With the Election Code (Counts III & VII)....40

a. The Election Code Requires Security Testing, Not Blind Reliance on Out Of Date ITA Reports That Were Not Even Reliable When Made 40

b. Even If ITA Testing Were Reliable, It Is Arbitrary And Capricious To Rely On Tests That Predate The Discovery of New Vulnerabilities 42

c. Mr. Cobb's Purported "Penetration Analysis" Was So Superficial That It Did Not Satisfy The Election Code In Any Meaningful Way 44

4. There Is A Genuine Issue of Material Fact Concerning Whether Respondent Has Violated The Pennsylvania Constitution (Counts VII, IX & X) 46

a. Respondent Misstates The Nature of Petitioners' Claims and Overstates The Effect of The Prior Summary Judgment Ruling 47

b. Respondent Misstates The Applicable Legal Standard 48

c. Respondent Misunderstands Which Facts Are "Material" 52

d. Respondent Ignores Genuine Disputes Concerning The Material Facts 54

V. CONCLUSION 57

TABLE OF AUTHORITIES

Page(s)

CASES

Allstate Life Ins. Co. v. Commw.,
992 A.2d 910 (Pa. Commw. Ct. 2010) 49

Applewhite v. Commw.,
No. 330 MD 2012, 2012 WL 3332376 (Pa. Commw. Ct. Aug. 15, 2012) 23

Applewhite v. Commw.,
54 A.3d 1, 3 (Pa. 2012) 49

Assoc. of Pa. State Coll. and Univ. Faculties v. Pa. Labor Relations Bd.,
607 Pa. 461, 8 A.3d 300, 304-05 (2010) 22

Banfield v. Aichele,
51 A.3d 300, 305 (Pa. Commw. Ct. 2012) ("*Banfield II*") 24

Banfield v. Cortes,
922 A.2d 36 (Pa. Commw. Ct. 2007) ("Banfield I") ..... *passim*

Borough of Nanty-Glo v. American Surety Co. of N.Y.,
309 Pa. 236, 163 A. 523 (1932) 2

Bowen v. Georgetown Univ. Hosp.,
488 U.S. 204 (1988) 26

Burdick v. Takushi,
504 U.S. 428 (1992) 50

Bush v. Gore,
531 U.S. 98 (2000) 50

Chem. Mfrs. Ass'n v. Natural Res. Def. Council, Inc.,
470 U.S. 116 (1985) 25

Christianson v. Colt Indus. Operating Corp.,
486 U.S. 800 (1988) 19

Commonwealth v. Starr,
541 Pa. 564, 664 A.2d 1326 (1995) 19

Dechert LLP v. Com.,
606 Pa. 334, 998 A.2d 575 (2010) 25, 26

DePaul v. Commonwealth,
600 Pa. 573, 969 A.2d 536 (2009) 51

Ducjai v. Dennis,
540 Pa. 103, 656 A.2d 102 (1995), *overruled in part on other grounds*, *Gardner v. Erie Ins. Co.*, 555 Pa. 59, 772 A.2d 1041 (1999) 2

Erfer v. Commw.,
568 Pa. 128, 794 A.2d 325 (2002) 50

Finucane v. Pa. Milk Mktg. Bd.,
136 Pa. Cmwlth. 272, 582 A.2d 1152 (1990) 50

FONNER V. SHANDON, INC.,
555 PA. 370, 724 A.2D 903 (1999) 30

In re Gen. Election for Twp. Supervisor,
152 Pa. Commw. 590, 620 A.2d 565 (Pa. Commw. Ct. 1993) 55

Hodosh v. Block Drug Co.,
786 F.2d 1136 (Fed. Cir. 1986) 2

Holt v. 2011 Legislative Reapportionment Comm'n
39 A.3d 711 (Pa. 2012) 49

In re Howells,
20 A.3d 617, 623 (Pa. Commw. Ct. 2011) 49

Ins. Adjustment Bureau v. Ins. Comm'r,
518 Pa. 210, 542 A.2d 1317 (1988) 52

James v. Se. Pa. Transp. Auth.,
505 Pa. 137, 477 A.2d 1302 (1984) 51

Keystone Redevelopment Partners, LLC v. Pa. Gaming Control Bd.,
5 A.3d 448, 461 (Pa. Commw. Ct. 2010) 22

Koken v. Commw. Professional Group,
2006 WL 334787 (Pa. Com. Pl. 2006) 2

Kuznik v. Westmoreland Cnty. Bd. of Comm'rs,
588 Pa. 95, 902 A.2d 476 (2006) 26, 50

Marks v. Tasman,
527 Pa. 132, 589 A.2d 205 (1991) 2

Masland v. Bachman,
473 Pa. 280 (1977) 41

Minick v. United States,
506 A.2d 1115 (D.C. 1986) 19

Mixon v. Commw.,
759 A.2d 442 (Pa. Commw. Ct. 2000), *aff'd*, 566 Pa. 616, 783 A.2d 763 (2001) 51

Nationwide Mut. Ins. Co. v. Foster,
143 Pa. Cmwlth. 433, 599 A.2d 267 (1991) 26

In re Nomination Papers of Rogers,
908 A.2d 948 (Pa. Commw. Ct. 2006) 50

Appeal of Norwood,
382 Pa. 547, 116 A.2d 552 (1955) 49

Page v. Allen,
58 Pa. 338 (1868) 49

Pennsylvania State Univ. v. Cnty. of Centre,
532 Pa. 142, 615 A.2d 303 (1992) 2

Perles v. Cnty. Return Bd. Of Northumberland,
415 Pa. 154, 202 A.2d 538 (1964) 51

Saenz v. Roe,
526 U.S. 489 (1999) 56

In re Sale of Real Estate by Lackawanna Co. Tax Claim Bureau,
22 A.3d 308, 316 (Pa. Commw. Ct. 2011) 41

Schade v. Maryland State Bd. of Elections,
401 Md. 1 (2007) 52

Seeton v. Adams,
50 A.3d 268, 276 (Pa. Commw. Ct. 2012) 22

Seeton v. Pa. Game Comm'n,
594 Pa. 563, 937 A.2d 1028 (2007) 24

St. Elizabeth's Child Care Ctr. v. Dep't of Pub. Welfare,
600 Pa. 131, 963 A.2d 1274 (2009) 26

Sweeney v. Tucker,
473 Pa. 493, 375 A.2d 698 (1977) 20

Tritt v. Cortes,
578 Pa. 317, 851 A.2d 903 (2004) 24

U.S. v. Utah Constr. & Mining Co.,
384 U.S. 394 (1966) 3

Weber v. Shelley,
347 F.3d 1101 (9th Cir. 2003) 52

Wexler v. Lepore,
87 So.2d 1276 (Fla Dist. Ct. App. 4th Dist. 2004) 52

In re Zulick,
832 A.2d 572 (Pa. Commw. Ct. 2003), *aff'd*, 575 Pa. 140, 834 A.2d 1126 (2003) 50, 51

CONSTITIUTIONS

Pa. Const. art. I, § 5 ..... 46, 49, 52

Pa. Const. art. VII, § 6 ..... 47, 49

STATUTES, RULES & REGULATIONS

42 U.S.C. § 15301 *et seq.* [Help America Vote Act (HAVA) 8

42 U.S.C. § 15484 41

FLA. STAT, Chapter 101 § 56075 (2012) 52

MD. CODE. ANN. ELEC. § 9-102 (2012) 52

1 Pa. Cons. Stat. Ann. § 1921 ..... 24, 25

25 Pa. Stat. Ann. § 3031.1 ..... 7, 34

25 Pa. Stat. Ann. § 3031.5 ..... 10, 37, 40, 41

25 Pa. Stat. Ann. § 3031.7 ..... *passim*

Pa.R.A.P. 1532 2

Pa.R.A.P. 1551 ..... 3, 4

Pa.R.A.P. 1517 3

Pa.R.C.P. No. 1035.2(1) 2

CAL. ELEC. CODE § 19250 (2012) 52

OTHER AUTHORITIES

Black's Law Dictionary (9th ed. 2009) 3

Candice Hoke, *Chapter 17: Voting Technology and the Quest for Trustworthy Elections, in America Votes! A Guide to Modern Election Law & Voting*, Section I: Background: Performance Records of E-Voting Systems, at n.22 (Benjamin E. Griffith, 2nd ed. 2012), available on Westlaw at ABA-AMVOTE § 17.1… 34-35

I. INTRODUCTION

In August 2011, the parties filed cross-motions for summary judgment. Petitioners' Motion turned on disputed legal questions but undisputed factual ones. Respondent's Motion, on the other hand, claimed there was no evidence anywhere in the record that supported any of Petitioners' claims. No doubt skeptical that every material fact in the case was really undisputed, President Judge Pelligrini scheduled briefing and argument on Petitioners' legal Motion and held Respondent's factual Motion in abeyance. *See* Order of August 17, 2011 (attached as Ex. 5 to Resp't's Supp. Br.).

As it happens, Judge Pelligrini was right; many of the material facts concerning whether Respondent certified DREs that prevent tampering with ballots or tabulating elements (Count II), whether her testing procedures ensured compliance with the Election Code (Counts III and VII), and whether her certification of the DREs was consistent with the Pennsylvania Constitution (Counts VII, IX and X) are very much in dispute. A casual reading of Respondent's brief might suggest otherwise, but that is because it focuses on undisputed facts that are not material and ignores disputed facts that are. For example, in seeking summary judgment on Petitioners' security claims under Sections 3031.7(17)(i) and 3031.7(16)(iii), Respondent argues that DREs have not been tampered with in an actual election in Pennsylvania (which is not a material fact) and points only to her expert's opinion that vulnerabilities cannot be exploited in "real elections" (which is also immaterial and in any event ignores the contrary opinions of Petitioners' experts and other notable experts in the field). *See* Resp't's Supp. Br. at 40.

Respondent may well believe that her expert is more credible than Petitioners' experts. Her expert's prior inconsistent statements suggest otherwise, but she is entitled to believe that. She is not, however, entitled to pretend that Petitioners' experts do not exist or do not disagree.

Fairly read, the record reveals a number of genuine issues of material fact that should preclude the entry of summary judgment. It follows that the Respondent's Motion should be denied.

II. STANDARD AND SCOPE OF REVIEW

A. Standard of Review

The parties agree on the appropriate standard of review: applications for summary relief pursuant to Pennsylvania Rule of Appellate Procedure 1532 are subject to the same standard of review as motions for summary judgment filed pursuant to Pennsylvania Rule of Civil Procedure 1035, which requires the movant to demonstrate that there are no genuine issues of material fact. *See* Pa.R.A.P. 1532, note (b); Pa.R.C.P. No. 1035.2(1). The parties also agree that the Court must review the record in the light most favorable to the non-movant, *see Marks v. Tasman*, 527 Pa. 132, 134-35, 589 A.2d 205, 206 (1991), and resolve all doubts against the movant. *See Pennsylvania State Univ. v. Cnty. of Centre*, 532 Pa. 142, 144-45, 615 A.2d 303, 304 (1992). In short, summary judgment is appropriate only if the movant's right to relief is free from doubt. *See* Pa.R.A.P. 1532(b); *see also Ducjai v. Dennis*, 540 Pa. 103, 113, 656 A.2d 102, 107 (1995), *overruled in part on other grounds*, *Gardner v. Erie Ins. Co.*, 555 Pa. 59, 772 A.2d 1041 (1999). A movant's right to relief is not clear if it supports its motion only with its own testimony, *see Borough of Nanty-Glo v. American Surety Co. of N.Y.*, 309 Pa. 236, 238, 163 A. 523, 524 (1932), or if the non-movant presents conflicting testimony on a material issue such that witness credibility must be weighed. *See, e.g.*, *Koken v. Commw. Professional Group*, 2006 WL 334787, at *2 (Pa. Com. Pl. 2006) (citing *Nanty-Glo*); *Hodosh v. Block Drug Co.*, 786 F.2d 1136, 1143 (Fed. Cir. 1986) ("The fact issues herein must be resolved by trial in which the conflicting views of the experts will be subject to the refining fire of cross-examination.").

B. Scope of Review

The parties disagree on the appropriate scope of review. Petitioners submit that, as this action is addressed to the Court's original jurisdiction, the scope of the Court's review is plenary. *See, e.g.*, Pa.R.App.P. 1517 ("[T]he practice and procedure under this chapter relating to pleadings in original jurisdiction petition for review practice shall be in accordance with the appropriate Pennsylvania Rules of Civil Procedure...."); Pa.R.App.P. 1551(b) ("Scope of Review . . . The court shall hear and decide original jurisdiction petitions for review in accordance with law. This chapter is not intended to . . . abridge the rights of any party to an original jurisdiction petition for review."); *id.*, Note ("[T]he appellate judge should inquire: 'Assuming that this case had been properly brought before me by a complaint ..., to what relief, if any, would the moving party have been entitled ...?").

Respondent has argued otherwise, however, claiming that the Court's review is "limited" to whether her "adjudication" was "in accordance with law" and based on "substantial evidence." Resp't's Appl. for Summ. Relief ¶ 13; *see also* Resp't's Supp. Br. at 5. Respondent is wrong, however, as her examination and certification of these DREs had none of the trappings of a judicial or even quasi-judicial adjudication (i.e., testimony under oath, an opportunity for anyone to present or cross-examine witnesses or object to evidence, an allocation of the burden of proof, etc.) such that the scope of this Court's review would be limited. *See, e.g.*, Black's Law Dictionary 47 (9th ed. 2009) ("Adjudication . . . 1. The legal process of resolving a dispute; the process of judicially deciding a case."); *U.S. v. Utah Constr. & Mining Co.*, 384 U.S. 394, 422 (1966) (noting that administrative adjudications can have preclusive effect if an agency acts "in a judicial capacity and resolve[s] disputed issues of fact properly before it which the parties have had an adequate opportunity to litigate"); *cf.* Pa.R.A.P. 1551(a) ("Review of quasijudicial orders

shall be conducted by the court on the record made before the government unit."). It follows that the scope of this Court's review is plenary.

Respondent also argues, under the rubric of the "scope of review," that this Court should defer to her because this case involves her interpretations of the Election Code, *see* Respondent's Supp. Brief in Supp. of Appl. for Summ. Relief at 4-5, or conduct that is discretionary. *Id.* at 6. Strictly speaking, however, whether this Court can or should defer to Respondent concerns the merits of Petitioners' claims. It has nothing to do with the "scope" of this Court's review, that is, what evidence this Court can or should consider in deciding the merits of those claims. Petitioners will therefore dispose of these arguments below.

III. BACKGROUND

A. The General Assembly Repeatedly Rejects Bills That Would Have Allowed EVSs But Not Required That They Create Recountable Records and Preclude Tampering

Respondent makes no mention of the relevant statutory provisions' legislative history. Indeed, her expert appears to believe there is no legislative history at all. *See* Shamos Rebuttal Report ¶ 47 (attached as Ex. 8 to Resp't's Supp. Br.) ("The 'authors' of the statute were the voting system vendors themselves."). On the contrary, there is an extensive legislative history, and it is one that, perhaps unbeknownst to Respondent, contradicts virtually every position she has taken throughout the course of this litigation.

The statutory provisions that allowed electronic voting systems ("EVSs") were added to the Election Code in 1980. *See* Act Amending the Pennsylvania Election Code, P.L. 600, No. 128 (Pa. 1980). The 1980 amendments were not the first drafts of those provisions, however. Rather, the legislative process started nearly a decade earlier with HB1366, which was introduced by Representative Harold Comer on July 26, 1971. *See* H.B. 1366, 1971 Gen. Assemb., Reg. Sess. (Pa. 1971) (attached hereto as Ex. 1). HB1366 did not require that EVSs

create permanent physical records, be subjected to an automatic statistical recounts, be examined and certified by the Secretary, or be designed such that they precluded tampering. *Id.*

HB1366 did not become law. Why? Because people who were familiar with computers refused to support it or substantially similar bills that were introduced in the following years. Notably, Representative Lee Taddonio, who had a background in computer science, objected because he believed EVSs were untested, unreliable, and unsafe. *See, e.g.*, Legislative Journal – House, at 5249 (Vol. 1 No. 152, June 25, 1974) (Statement of Rep. Taddonio) (attached hereto as Ex. 2) ("[T]he point was made by the gentleman from Cambria that the system was tested and true. I disagree with that."); Legislative Journal – House, at 5302-05 (Vol. 1 No. 153, June 26, 1974) (attached hereto as Ex. 3) ("Yesterday we put in some amendments, which I believe strengthen the bill. However, there are some weaknesses in the system which I think should be brought to light.... What are the problems? There are certain areas I wish to address. First of all, there are the possibilities of fraud. 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 one of two things: One, that the fraud is there but it has not been discovered. In other words, it could be impossible to detect. Two, it could be that because of the technology the individuals who wish to be dishonest have not yet educated themselves or become placed in the right position.... We are tampering with the very basis of democracy. 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."); *id.* at 5305 ("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."); *id.* at 5307 (statement of Rep. Dreibelbis) (arguing in favor of amendment but noting that EVSs should be "made hopefully as fool-proof as possible.");

Legislative Journal – House, at 2040-41 (No. 55, July 2, 1980) (Statement of Rep. Taddonio) (attached hereto as Ex. 4) ("Mr. Speaker, this bill has been around for at least 8 years, since I have been here in this General Assembly, and it has failed to pass in all those 8 years.... I think there is a very good reason for that.... This is a very extensive change to our Election Code to allow what they call computerized voting machines. This change, in my opinion, would open up the door and the floodgates to a lot of potential fraud. My background is in the computer field. I have worked in that area most of my working life.... This legislation, in my opinion, is premature, and, even if that, it still is defective.... 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. This bill keeps coming around. 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. It is not infallible, and if someone is sophisticated enough to defraud the system, they are also sophisticated enough to influence that sample so that it will come out correctly...."). Notably, Representative Taddonio and others had those concerns even though every commercially viable EVS at that time was a punch card or optical scan system that, unlike DREs, necessarily created a recountable record of every individual vote the moment it was cast.[1] (The Shouptronic ELECTronic received U.S. Patent No. 4,641,240 in 1987.)

---

[1] *See, e.g.*, Memorandum from W. Boehm to D. Cooper dated Dec. 14, 2006, at 7 (attached hereto as Ex. 31) ("Act 128 was drafted during an era when electronic voting systems were largely punch card voting systems. DRE's [sic] were not yet on the market but were in development. ***The language of Act 128 contains a very heavy bias toward systems using punch cards (now replaced) or optical scan 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.") (emphasis added).

It was not until 1980 – after the bill was amended so that it required that EVSs create "permanent physical records," be subjected to an automatic "statistical recount," be examined and certified by the Secretary, and be designed in a way that precluded "every person" from tampering with them – that the General Assembly allowed EVSs to be used in elections. *See* 25 P.S. §§ 3031.1, 3031.17, 3031.7(17)(i). It is against that backdrop that the parties' competing statutory interpretations must be viewed.

B. The General Assembly's Concerns About The Security and Reliability of EVSs Were Shared By Scientists Who Were Familiar With Electronic Voting

The General Assembly's desire that EVSs be as secure as possible were by no means unique at the time it amended the Election Code. On the contrary, its concerns were shared by many others who were familiar with computers—including at least one of the people Respondent would later retain to examine EVSs and offer expert opinion testimony in this case.

Indeed, a full eight years ***after*** the Election Code was amended to allow EVSs to be used in Pennsylvania elections, Dr. Michael Shamos cautioned that they were susceptible to undetectable tampering. 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." Ronnie Dugger, *Annals of Democracy – Counting Votes*, The New Yorker (Nov. 7, 1988) (attached hereto as Ex. 5) at P-15175. He dismissed the idea that large-scale fraud requires a large-scale operation. On the contrary, he said it could be accomplished by "[o]ne person. The point is that, the way things are going, a national mechanism exists that could be manipulated by anybody, from a single individual to a nationwide conspiracy." *Id.* at P-15195; *see also id.* at P-15183 ("[T]he possibility exists that an unauthorized person may gain access to the central point from which these programs are distributed and alter them. The implications are frightening

when it is remembered that one-quarter of all votes cast in the U.S. are counted by these programs."). He also rejected the suggestion that fraud could be detected after the fact: "Computerized 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.***" *Id.* at P-15195 (emphasis added).

C. Respondent Certifies DREs For Use In Commonwealth Elections Despite Having Conducted No Meaningful Security Tests Of Her Own

In October 2002, the Help America Vote Act (HAVA), 42 U.S.C. § 15301 *et seq.* was enacted in response to the controversy surrounding the November 2000 presidential election. HAVA allocated a significant amount of federal funding to the States for complying with its requirements, most notably the replacement of lever voting machines and punched card systems. In order to receive federal funds, Pennsylvania was required to comply with HAVA by the first federal election after January 1, 2006. *See* Pennsylvania State Plan, as amended 2005 (attached hereto as Ex. 6), at 1-2 & Element 12 at 54. As that deadline approached, it was "all hands on deck" for Respondent.[2] Indeed, as then-Secretary Cortes candidly observed at the time, "[e]very day that goes by without additional certified systems puts the Commonwealth, particularly the Department, in a terribly [sic] predicament." Email to Kenneth Rapp dated September 19, 2005 (attached hereto as Ex. 8). It was "in the context [that] deadline," which put "millions in federal funds" at risk, that Respondent certified DREs for use in Commonwealth elections. Resp't's Br. in Supp. of Preliminary Objections at 24 & 4 n.3.

---

2 *See* Marks Dep. (excerpts attached hereto as Ex. 7) at 22.

The DREs at issue in this case were examined by either Dr. Shamos or Glenn Newkirk in late 2005 and early 2006. Notably, they did not review any source code,[3] and did not conduct any meaningful penetration analysis to determine whether election results could be altered. Instead, they simply relied on independent testing authorities ("ITAs") to do that work.[4] Never mind that Dr. Shamos testified that ITA testing is inadequate,[5] and had stated at that time that the ITA testing process was "dysfunctional" and "not only broken, but virtually nonexistent."[6] As he put it, Pennsylvania had simply "abdicated" its obligation to conduct meaningful security testing:

> [T]he current process of qualification testing by Independent Testing Authorities ... is not effective. As proof I need only cite the fact that the voting systems about which security concerns have recently been raised, such as Diebold Accuvote, were all ITA-qualified. Some of these systems contain security holes so glaring that one wonders what the ITA was looking for during its testing.... The next step after qualification, certification to individual state requirements, is also flawed. Many states that formerly had statutory certification procedures have

---

3 Shamos Dep. (attached hereto as Ex. 9) at 76 (noting with respect to ES&S exam he had the source code available but does not recall whether actually looked at it) (Ex. 4); *Id.* at 106 (noting had source code but does not recall if he looked at it in connection with Diebold examination); Newkirk Dep. (excerpts attached hereto as Ex. 10) at 166-67 (stating he did not review source code in connection with Hart examination) ; *Id.* at 253 (did not review source code in connection with Danaher re-examination).

4 Shamos Dep. (Ex. 9) at 86 ("That's the whole point of the ITA system, is to avoid having the states repetitively test the same thing 50 times that the ITA could test once."); Marks Dep. (Ex. 8) at 197 (noting ITA report used by examiner as resource in preparing examination report); Newkirk Dep. (Ex. 10) at 170-71 (noting relying upon source code analysis in ITA reports); *id.* at 186-87 (noting didn't examine particular security issue with removable cartridges because that security analysis was within scope of ITA review).

5 Shamos Dep. (Ex. 9) at 27 ("[t]oo many systems pass ITA qualifications that shouldn't"); *Id.* at 30-31 ("[w]hen a system comes for certification in Pennsylvania, the only flaws that it should conceivably have are failure to comply with Pennsylvania procedures, the way we count votes in Pennsylvania. I shouldn't find flaws that ought to have been detected by the ITA, yet I did. So that suggested to me that the ITA process wasn't adequate."); *id.* at 47 (agreeing that *additional testing beyond ITA certification is needed to test the security of DREs before they're used in an election.*); *see also supra* note 5.

6 Testimony of Michael I. Shamos before the Environment, Technology, and Standards Subcommittee of the U.S. House of Representatives' Committee on Science dated June 24, 2004 ("Shamos 2004 Testimony," attached hereto as Ex. 11) at 1.

> abdicated them in favor of requiring no more from a vendor than an ITA qualification letter.... My own state, Pennsylvania, abandoned certification in 2002 because it believed the ITA process was sufficient. We are less safe in 2004 than we were 20 years ago.

Shamos 2004 Testimony (Ex. 11) at 1. In any event, Respondent's examinations were the equivalent of kicking the tires to test the car – examinations of a few things by a few people for a few hours and reliance on an ITA process the examiners knew were unreliable.

D. Respondent Refuses To Reexamine DREs Despite A Growing Consensus That They Do Not Prevent Every Person From Tampering With Them

In January, March and April 2006, Petitioners and others requested reexaminations. Their requests were signed by ten or more registered electors and included a check in the amount of the reexamination fee as required by 25 Pa. Stat. Ann. § 3031.5; however, those requests were denied.[7] Indeed, it was not until five years later – perhaps not coincidentally on the eve of the deadline for filing summary judgment motions – that Respondent reversed course and announced her intention to reexamine the DREs at some unspecified time in the future.[8] In the interim, Respondent ignored a growing consensus that DREs had serious security vulnerabilities.

1. 2005 Report of the Brennan Center Task Force on Voting System Security

In 2005, the Brennan Center for Justice (a non-partisan public policy and law institute that focuses on the fundamental issues of democracy and justice) convened a task force of "government, academics, and private-sector scientists, voting machine experts and security professionals to conduct the nation's first systematic analysis of security vulnerabilities in the three most commonly purchased electronic voting systems." Brennan Study (attached hereto as Ex. 14) at P-13910. Several DREs that are at issue here (specifically the Sequoia AVC Edge, the

---

7 *See* Letters from P. Cortes (attached hereto collectively as Ex. 12).

8 *See* Letter from C. Aichele (attached as Ex. 13).

Sequoia AVC Advantage, the ES&S iVotronic and the Diebold Accuvote-TSx) were examined. The task force concluded that the machines "do not have available to them a powerful countermeasure to software attacks," which is particularly problematic for DREs because they do not have "voter-verified paper trails...." *Id.* at 4. It also found that, with respect to DREs, "when the goal is to change the outcome of a close statewide election, attacks that involve the insertion of Software Attack Programs or other corrupt software are the least difficult attacks." *Id.* at 3. Notably, it made clear that these security vulnerabilities were applicable to a real election: "[t]here is no reason why the methods used in this analysis cannot be applied to local (or national) races." *Id.* at 2.

2. 2006 Halderman Report on Security Analysis of the Diebold AccuVote-TS

In 2006, computer scientists from Princeton University analyzed security vulnerabilities associated with the AccuVote TS, the predecessor of the AccuVote TSx used in Pennsylvania. *See* Security Analysis of the Diebold AccuVote-TS Voting Machine ("the Halderman Report," attached hereto as Ex. 15). This study analyzed the machine's hardware and software and "considered whether real election practices would leave it suitably secure." *Id.* at 1. It 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." *Id.* As part of this study, the authors conducted several attacks that could be performed in a real election. The attacks were divided into two categories: vote stealing attacks and injecting attack code. *Id.* at 3-4. With respect to injecting attack code, the author explained how malicious code can be installed on one or more machines in less than one minute, *id.* at 4, and how malicious code could then be spread from one machine to another. *Id.* at 5. Ultimately, they concluded that:

> DREs may resist small-scale fraud as well as, or better than, older voting technologies; but 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.
>
> Electronic voting machines have their advantages, but experience with the AccuVote-TS and other paperless DREs shows that they are prone to very serious vulnerabilities. Making them safe, given the limitations of today's technology, will require safeguards beginning with a voter-verifiable paper audit trail and truly independent security evaluation.

Id. at p. 17.[9]

3. 2007 Report of Florida State University Information Technology Laboratory

In 2007, Florida's Secretary of State issued a report based on independent testing by the SAIT laboratory as part of Florida's voting system certification process. *See* Software Review and Security Analysis of the Diebold Voting Machine Software, available at www.cs.jhu.edu/~rubin/SAIT.pdf "FL SAIT Report"; *see also* Supplemental Florida SAIT Report, attached hereto as Ex. 17. The report concerned a newer version of the Diebold AccuVote TSx and the same version of the GEMS software used in Pennsylvania.[10] The report highlighted the following attack scenario:

---

[9] *See also, e.g.*, Aviel D. Rubin, Ph.D., *Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting* 2005 (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 time 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 in recent years."). Notably, Respondent's expert once said much the same. *See* Tr. of Hearing Before the Texas House Committee on Elections (Nov. 25, 1986) (attached hereto as Ex. 16) at P-15748 ("There is the 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. ***The possibility of manipulation on such a grand scale does not exist with paper ballots or with lever machines.***") (emphasis added).

[10] The Florida SAIT also performed a Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware in connection with Florida's audit of the 2007 Florida Congressional District 13 election. Full Report available at

(Continued)

> an attack that allows an adversary to prepare official, activated voter smart cards that would enable voters to cast multiple ballots in a ballot-stuffing attack. Creation of the cards require 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 (these steps could be done by separate adversaries.) 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 or thus cannot be removed.

Id. at 3-4. This attack was contemplated to be carried out in a real election. *See id.*

4. 2007 California Top to Bottom Report

California conducted a "Top to Bottom Review" of certain DREs in 2007. That review involved source code review and penetration analyses that were significantly more thorough than anything that had ever been conducted in Pennsylvania at that time – or since, for that matter. The review uncovered numerous security concerns that ultimately caused California's Secretary of State to decertify the Diebold AccuVote TSx DRE, the Hart Intercivic eSlate DRE and the Sequoia AVC Edge 2. For example, the review detailed an attack on the Diebold in which 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." Lopresti Supp. Report (attached hereto as Ex. 18) at 7. With respect to the Hart Intercivic eSlate DRE, the review determined that "software running on the Hart system often fails to check the validity

---

(Continued)

http://nob.cs.ucdavis.edu/bishop/notes/2007-fsusait-1/2007-es+s.pdf. Dr. Shamos was among the investigators involved with this Study. Although the investigators determined that the firmware on the iVotronic did not cause the undervote issue present in the election, the examiners identified several other security vulnerabilities with the iVotronic firmware. *Id.* at § 7 ("Our security findings relate to external data in four areas: PEBs, Compact Flash cards, modem operations, and password handling. External communications are natural targets that intruders might try to attack."). Many of these vulnerabilities overlap with the findings of the Ohio Everest Report and were still present when the iVotronic was subjected to testing in Ohio.

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." *Id.* (Hart Source Code Review). And with respect to the Sequoia AVC Edge 2, the review "determined that the Sequoia Edge firmware includes a shell-like scripting language, interpreter, in apparent violation of Section 4.2.2 of the 2002 Voting Systems Standards, which provides commands for setting the supposedly tamper-proof protective counter of the machine, setting the machine's serial number, overwriting other software and firmware in the system (including the audit trail), and rebooting the machine at will (p. 7 of "Security of the Sequoia Voting System")." *Id.* at 7; *see also* Excerpts from California Top to Bottom Review (attached hereto as Ex. 19, and full report available online at http://www.sos.ca.gov/voting-systems/oversight/top-to-bottom-review.htm) at 15. Subsequently, California conditionally recertified certain systems for use in limited circumstances such as with voting by persons with disabilities as long as enhanced security measures and post-election audit procedures were observed.

5. The 2007 Ohio EVEREST Report

Similarly, the Ohio EVEREST study conducted by the State of Ohio in 2007 caused the Ohio Secretary of State to recommend that all DREs be decertified in Ohio. Like the California Top to Bottom Review, the Ohio EVEREST study was more thorough than any examination ever performed in Pennsylvania. With respect to the Diebold AccuVote TSx, "the Ohio examiners found that buffer overflows – a common type of programming error – present in the Premier software can be exploited by an attacker to run arbitrary code on the DRE which can then propagate to other components in the election system, including the GEMS server." 2008 Lopresti Report, Ex. 24 at ¶ 17(c)(i) (referencing pp. 4-5 of Everest Project Premier System Technical Details Report), available at http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf) (full Ohio EVEREST Report); see also Excerpts from

Ohio EVEREST Report (attached hereto as Ex. 20). With respect to the eSlate, "the Ohio examiners found that the Judges Booth Controller, which administers the DRE units, generates supposedly 'random' voter access codes that are easy to predict after viewing a small number of past codes. Exploiting this vulnerability would allow an attacker to vote multiple times using the DRE." *Id.* at ¶ 17(c)(ii) (referencing p. 11 Everest Project Hart System Technical Manager Report), available at http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf). And with respect to the ES&S iVotronic, "[t]he Ohio examiners found that the iVotronic can be rebooted by a voter with the use of a simple magnet . . . . At best, this would make the machine unusable for a period of time – the modern day equivalent of locking voters out of the polling place." *Id.* at ¶ 17(c)(iii) (referencing p. 5 Everest Project ES&S System Technical Details Report), available at http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf).

6. 2011 Testing by the Argonne National Laboratory

In 2011, Dr. Roger Johnston, the head of the Vulnerability Assessment Team at the Argonne National Laboratory (a non-profit research laboratory operated by the University of Chicago for the Department of Energy) demonstrated how to perform a "man in the middle" attack on an AccuVote TSx and a Sequoia AVC Advantage during an actual election with less than $30 of equipment from Radio Shack, a basic understanding of electronics and less than one minute alone inside the voting booth. As a result of the attack, he could manipulate subsequent votes on the DREs in a way that would be invisible to voters and undetectable to election officials. He described the attack as follows:

> 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. We're basically interfering with transmitting the voter's intent.

> We used a logic analyzer. Digital communication is a series of zeros and ones. The voltage goes higher, the voltage goes lower. A logic analyzer collects the oscillating voltages between high and low and then will display for you the digital data in a variety of formats. But there are all kinds of way to do it. You can use a logic analyzer, you can use a microprocessor, you can use a computer—basically, anything that lets you see the information that's being exchanged and then lets you know what to do to mimic the information.
>
> ***I've been to high school science fairs where the kids had more sophisticated microprocessor projects.*** So we listened to the communications going on between the voter, who in the case of one machine is pushing buttons (it's a push-button voting machine) and in the other is touching things on a touchscreen. Then we listened to the communication going on between the smarts of the machine and the voter. Let's say I'm trying to make Jones win the election, and you might vote for Smith. Then my microprocessor is going to tell the smarts of the machine to vote for Jones if you try to vote for Smith. But if you're voting for Jones anyway, I'm not going to tamper with the communications. Sometimes you block communications, sometimes you tamper with information, sometimes you just look at it and let it pass on through. That's essentially the idea. Figure out the communications going on, then tamper as needed, including with the information being sent back to the voter.

Roger Johnston, *This is How I Hacked an Electronic Voting Machine*, Popular Science (attached hereto as Ex. 21, and available online at http://m.popsci.com/gadgets/article/2012-11/how-i-hacked-electronic-voting-machine) (emphasis added). He concluded that "anyone who does digital electronics – a hobbyist or an electronics fan – could figure this out." *Id.*

7. Petitioners' Expert Reports and Expert Testimony In This Proceeding

Petitioners' experts, Dr. Jones and Dr. Lopresti, testified that the DREs at issue in this case suffer from serious security vulnerabilities. For example, they cautioned that the DREs do not preclude tampering with the tabulating element. *See, e.g.*, Jones 2011 Report (attached hereto as Ex. 23) ¶ 95 (explaining that malicious code can be injected into DRE to change tabulation); 2008 Jones Report (attached hereto as Ex. 22) ¶ 36 (explaining that tampering with the PEB on the iVotronic can change tabulation). They have also explained how the DREs do not preclude tampering with ballots. *See, e.g.*, Jones 2008 Report (Ex. 22) ¶ 51 (explaining how memory cards can be used to tamper with ballots); Lopresti 2008 Report (attached hereto as Ex.

24) ¶ 17(b)(i) (explaining attack from California Top to Bottom Report involving deletion of ballots on Diebold TSx machine using a few easily concealed tools). They opined that these vulnerabilities pose real, not imagined or hypothetical, threats of tampering. *See, e.g.*, Jones 2008 Report (Ex. 22) ¶ 40 ("These defects are not merely of theoretical interest, the red-teams convened as part of the California TTBR and the Ohio Everest efforts were able to exploit the flaws found in every voting system that they tested in a way that could be used to corrupt an election."). They also testified that many of these attacks can go entirely undetected. *See, e.g.*, Lopresti 2011 Report (Ex. 18) at 9. Importantly, they opined that pre-election testing and other purported procedural safeguards are not necessarily effective at preventing or detecting fraud. *See, e.g.*, 2011 Jones Report (Ex. 23) ¶ 93 (noting that polling procedures cannot substitute for security measures); 2008 Jones Report (Ex. 22) ¶ 57 (noting in some cases there are no feasible procedural defenses).

E. Respondent Eventually Reexamines DREs But Still Fails To Test Whether DREs Preclude Tampering With Ballots or Tabulating Elements

Respondent, Dr. Shamos and Mr. Newkirk were familiar with the Ohio EVEREST report and California's Top to Bottom Review when they were issued.[11] Indeed, Dr. Shamos admitted that those reports "raise important security issues" and that "the evidence adduced by California and Ohio should be considered by the Secretary" in deciding "which remediations of the identified systems might be undertaken to counteract their security vulnerabilities." Shamos Report (attached as Ex. 7 to Resp't's Supp. Br.) ¶¶ 91, 126; *see also* He aring before the Committee on House Administration, Hearing On Verification, Security And Paper Records For Our Nation's Electronic Voting Systems (Sept. 28, 2006) (attached hereto as Ex. 26) at P-15339

[11] Newkirk Dep. (Ex. 10) at 213-17; Shamos Dep. (Ex. 11) at 258-59; Marks Dep. (Ex. 7) at 226-32.

("Professor Felten at Princeton, Harri Hursti, and others have done a great service by exposing security vulnerabilities in voting systems. Some of these vulnerabilities are severe and require immediate repair....") (quoting Dr. Shamos). Nevertheless, Respondent took no steps to reexamine DREs after those reports were issued.[12]

What's more, when Respondent finally decided to reexamine these DREs in order to moot Petitioners' request for a court order directing her to do so, she retained a new examiner who had only a vague understanding of the California and Ohio reports and acknowledged that he did not consider them during his reexaminations. With respect to the other published reports documenting security vulnerabilities with DREs, Mr. Cobb had not even heard of these reports. *See* Ex. 30, Cobb Dep. at 131-132; 137; 205.

IV. ARGUMENT

A. Respondent's Legal Arguments Find No Support In The Law

Respondent has asserted a number of threshold legal defenses to Petitioners' claims, including sovereign immunity, the separation of powers, and deference of one form or another. If these defenses sound familiar, that is because they are; Respondent has raised all of them at some point throughout the course of this litigation and *en banc* panels of this Court either explicitly or implicitly rejected every one of them. The Court was right to do so before and should do so again now.

1. Respondent Is Not Immune From Petitioners' Suit, Which Simply Seeks to Compel Her to Carry Out Her Duties Pursuant to the Election Code

The question of whether Respondent is immune from this suit was answered long ago, as Respondent acknowledges in her brief. *See* Resp't's Supp. Br. at 47-48 ("a majority of this

---

12 Marks Dep. (Ex. 7) at 226-232.

Court noted that the Secretary is not immune from a lawsuit seeking mandamus relief."). Specifically, an *en banc* panel of this Court found that "the doctrine of sovereign immunity does not bar suits that seek to compel state officials to carry out their duties in a lawful manner." *Banfield v. Cortes*, 922 A.2d 36, 43 (Pa. Commw. Ct. 2007) ("Banfield I") (citations omitted). Respondent demeans that ruling as a "loophole" that is no longer available now that there has been discovery. Resp't's Supp. Br. at 48. She does not articulate why that would be, though, let alone how the record compels a different result. Nor could she.

The law of the case doctrine promotes finality and fairness by preventing the agitation of settled issues. Pursuant to that doctrine, the Court should reject Respondent's attempts to revisit its preliminary objection ruling. *See, e.g., Christianson v. Colt Indus. Operating Corp.*, 486 U.S. 800, 817 (1988) ("[A]s a rule courts should be loathe to [revisit prior decisions of its own or of a coordinate court] in the absence of extraordinary circumstances such as where the initial decision was clearly erroneous and would work a manifest injustice.") (internal quotation and citation omitted); *Commonwealth v. Starr*, 541 Pa. 564, 574, 664 A.2d 1326, 1331 (1995) (stating that issues should not be reopened "in the later phases of a litigated matter"). That is particularly true here, where the law of the case was set by an *en banc* panel. *Cf. Minick v. United States*, 506 A.2d 1115, 1116 (D.C. 1986) (stating that "a panel of this court is not a 'higher court' than [the] court sitting en banc," and concluding that the panel court was bound by the *en banc* panel's decision). It follows that the Court should reject this argument a second time and Respondent can make it a third time on appeal if necessary.

2. Compelling Officials To Comply With The Election Code Does Not Trigger, Let Alone Offend, The Separation of Powers Doctrine

Similarly, Respondent suggests that granting the relief Petitioners request would offend the separation of powers doctrine because, unlike this Court, the General Assembly is charged

with setting election policy and Respondent is charged with enforcing it. *See* Resp't's Supp. Br. at 45. The Court already rejected this argument as well, though, finding that it does not violate the separation of powers doctrine to interpret the law and direct officials to comply with it:

> In the fourth preliminary objection, the Secretary argues that Electors ask this Court to violate the separation of powers doctrine by usurping the power of the executive branch of government to de-certify electronic voting systems . . . and establish testing criteria. We disagree. The judicial branch does not usurp the power of the executive branch by interpreting and applying a legislative enactment and directing that the Secretary comply with it.

Banfield I, 922 A.2d at 44. A contrary rule would place virtually every executive action beyond review—an attractive notion for the government perhaps, but an untenable one for the governed.

Simply put, Petitioners are asking the Court only to direct Respondent to comply with the Election Code. If Respondent believes Petitioners have misread the Election Code in some way, that goes to the merits of their claims. It would not trigger the separation of powers doctrine. *See id.* Respondent's authority is not to the contrary. *See, e.g., Sweeney v. Tucker*, 473 Pa. 493, 507-22, 375 A.2d 698, 704-12 (1977) (reasoning that the expulsion of a legislator did not constitute a nonjusticiable political question).

3. The Court Can Grant All of the Relief Requested in the Petition, Including A Writ of Mandamus Compelling Compliance with the Election Code

Respondent argues that the Court should enter summary judgment in her favor because the Court does not have the authority to grant the injunctive relief requested in the Petition. *See* Resp't's Supp. Br. at 34-39. This argument fails for at least two reasons.

First, in addition to seeking injunctive relief, Petitioners also seek declaratory relief. *See* Petition (attached as Ex. 1 to Resp't's Supp. Br.) ¶¶ 114-15 (seeking a declaration that DREs do not satisfy Election Code requirements); *id.* ¶¶ 116-17, 129-30 (seeking any "further relief that this Honorable Court deems just and appropriate" concerning Respondent's testing procedures); *id.* at ¶¶ 131-44 (seeking declarations that DREs do not satisfy certain requirements of the

Pennsylvania Constitution). Respondent does not dispute that this Court can properly grant declaratory relief. It follows that Petitioners' claims should proceed even if the Court concludes that they do not satisfy the requirements for obtaining injunctive relief.

Second, Respondent made this same argument in her preliminary objections and this Court rejected it. Specifically, an *en banc* panel of this Court found that the Petitioners are able to obtain, and this Court is empowered to grant, a writ of mandamus to compel Respondent to perform "a ministerial act or mandatory duty where there exists a clear legal right in the plaintiff and a corresponding duty in the defendant and where there is no other adequate remedy at law." *Banfield I*, 922 A.2d at 42 (citation omitted). Furthermore, as this Court stated, a writ of mandamus may issue to compel the performance of purportedly discretionary acts "where the exercise or non-exercise of discretion is arbitrary, fraudulent, or based upon a mistaken view of the law." *Id.* (citation omitted).

Respondent suggests that the General Assembly vested her with discretion to decide not only the "results" of the statutory certification process, but also the "extent" of that process. *See* Resp't's Supp. Br. at 36. But as this Court already found, it cannot reasonably be disputed that Respondent is obliged to test for compliance with all of the requirements of the Election Code:

> [T]he Secretary argues that Electors are not entitled to mandamus relief because Electors do not have a clear right to have the Secretary establish uniform testing criteria that comply with the Election Code. However, section 1105-A of the Election Code states that, after each DRE examination, the Secretary shall file a report stating whether the DRE 'can be safely used by voters at elections as provided in this act and meets all of the requirements hereinafter set forth.' It would be impossible for the Secretary to file such a report if the Secretary did not establish uniform testing criteria that comply with the Election Code. To the extent that the Secretary believes that section 1105-A allows the Secretary to examine DREs without regard to the requirements of the Election Code, the Secretary is mistaken.

Banfield I, 922 A.2d at 42-43 (citations omitted).

Here, although the Election Code does not specify exactly ***how*** an EVS should be tested, it does specify exactly ***what*** should be tested. Put differently, the Election Code requires that Respondent test for ***all*** of its requirements, including those pertaining to security and tampering. Indeed, Respondent admits as much elsewhere in her brief. *See* Resp't's Supp. Br. at 36 (describing her "duty to 'examine and reexamine voting machines, and to approve or disapprove them for use in this state, in accordance with the provisions of [the Code].'") (citation omitted). Respondent did not do that, though. At best, that was a result of a misunderstanding of the law. At worst, it was arbitrary and capricious. *See, e.g., infra* Section IV.B.3.b. In either case, courts have the authority to issue appropriate relief, including a writ of mandamus. *See Assoc. of Pa. State Coll. and Univ. Faculties v. Pa. Labor Relations Bd.*, 607 Pa. 461, 469, 8 A.3d 300, 304-05 (2010); *Keystone Redevelopment Partners, LLC v. Pa. Gaming Control Bd.*, 5 A.3d 448, 461 (Pa. Commw. Ct. 2010).[13]

---

[13] Respondent cites *Seeton v. Adams*, 50 A.3d 268, 276 (Pa. Commw. Ct. 2012) for the proposition that discretionary actions can only be the subject of mandamus relief when the government official has not purported to exercise discretion at all. *See* Resp't's Supp. Br. at 35. *Seeton* is very different from this case, however, in that it involved prosecutors' time-honored discretion concerning not only how, but whether, to enforce the criminal code. There is no corresponding discretion concerning whether to enforce the Election Code. In any event, *Seeton* acknowledges that "there [is] in fact no actual exercise of discretion" when a public official acts "by a mistaken view of the law or by an arbitrary exercise of authority." *Seeton*, 50 A.3d at 274. It goes on to clarify that, "an official's refusal to exercise discretion could be intentional, *i.e.*, 'arbitrary,' or unintentional, *i.e.*, 'by a mistaken view of the law.' Whatever the reason for the official's refusal to exercise discretion, a writ of mandamus 'will lie' to compel the official to do so." *Id.* So too here. Respondent also cites *Seeton* for the proposition that a writ of mandamus will not lie simply because a public official exercised her discretion in a way that a complainant or court considers to be wrong, unwise or undesirable. *See* Resp't's Supp. Br. at 35-36; *see also id.* at 45 ("Petitioners . . . do not have a clear right to have examinations or reexaminations performed in a particular manner."). This argument is a distraction, as Petitioners have never asked the Court to order Respondent to exercise her discretion in any particular way other than in compliance with the Election Code. This argument is no more compelling now than it was when the Court rejected it six years ago. *See Banfield I*, 922 A.2d at 42 ("The Secretary also argues that Electors are not entitled to mandamus relief because Electors do not have a clear right to have the Secretary re-examine a DRE in a particular manner. However, Electors do not allege in their Petition that any Elector asked the Secretary to re-examine a DRE in a particular manner. Thus, we shall not consider this matter further.") (internal citation omitted).

We should not lose sight of the fact that this is 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. This is not a discretionary function, but one mandated by the Constitution. Respondent's defense is that she undertook some level of examination of the machines and that the proof of the adequacy of that examination is not that it passes scientific or even commercial banking standards of adequacy to withstand tampering, but that nothing bad has happened yet. That is the same defense that was raised against criticism of nuclear plant safety before the Fukushima Daiichi disaster demonstrated that "speculative" risks were nonetheless very real.[14]

It is clear from the Election Code's language and legislative history that the legislature recognized the importance of the right to vote, restricted the use of EVSs in elections to those machines that precluded tampering, and required Respondent to hold EVSs to that standard. There is an abundance of evidence that Respondent did not do that. On the contrary, it is indisputable that Respondent's reexaminer did not consult even one of the many studies (such as the Ohio EVEREST Report or the California Top to Bottom Review) that have revealed security vulnerabilities, much less try to determine whether those vulnerabilities could be exploited by real people in real elections. For their part, Petitioners' experts did review those studies, did find that those vulnerabilities continue to exist, and did determine they could be exploited in real elections. If anything, the record weighs in favor of entering summary judgment in favor of *Petitioners*. At a minimum, though, it certainly requires that it *not* be granted in favor of

---

[14] This is also the polar opposite of the stance Respondent has taken in the *Applewhite* case, in which she advocated in favor of strict voter identification rules due to the mere possibility that widespread voter identification fraud might one day be uncovered. *See, e.g.*, Respondents' Answer to Petitioners' First Set of Interrogatories *quoted in Applewhite v. Commw.*, No. 330 MD 2012, 2012 WL 3332376, at *27 (Pa. Commw. Ct. Aug. 15, 2012) *vacated* 54 A.3d 1 (Pa. 2012).

Respondent. Unless, that is, this Court is prepared—contrary to its *en banc* decision on the preliminary objections—to decide that her conduct here is unreviewable as a matter of law.

4. Respondent's Statutory Interpretations Are Not Entitled To Deference Because They Conflict With the Statute's Language and Legislative History

Respondent argues that the Court is obliged to defer to her statutory interpretations. *See* Resp't's Supp. Br. at 5-6, 45. She is wrong for at least four reasons.

First, deference to an agency's statutory interpretation is only necessary if the statute is vague or ambiguous. *See, e.g.*, 1 Pa. Con. Stat. Ann. § 1921(b); *Seeton v. Pa. Game Comm'n*, 594 Pa. 563, 578, 937 A.2d 1028, 1037 (2007) ("deference never comes into play when the statute is clear"); *Tritt v. Cortes*, 578 Pa. 317, 321, 851 A.2d 903, 905 (2004) ("an interpretation of a statute by those charged with its administration and enforcement is entitled to deference, [but] . . . such consideration most appropriately pertains to circumstances in which the provision is not explicit or is ambiguous.") (citations omitted). That is so even if the clear language leads to what Respondent deems to be an undesirable or even absurd result. *Cf.* 1 Pa. Cons. Stat. Ann. § 1921(b) ("When the words of a statute are clear and free from all ambiguity, the letter of it is not to be disregarded under the pretext of pursuing its spirit."). Here, while the last round of summary judgment briefing concerned undisputed facts and disputed statutory language,[15] this round concerns disputed facts and mostly undisputed statutory language. Indeed, Respondent's

---

[15] Notably, although the Court adopted Respondent's reading of the Election Code provisions that were at issue, it did not do so because of deference. Rather, it resolved the interpretative issues based on its own reading of the Election Code. *See, e.g., Banfield v. Aichele*, 51 A.3d 300, 305 (Pa. Commw. Ct. 2012) ("*Banfield II*") ("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."); *id.* at 307-08 ("We agree with the Secretary that the term must be construed in a manner which serves the purposes of the Election Code. Accordingly, we conclude that a permanent record is one that will remain stable or intact and be available for an indefinite period of time . . . .") (citation omitted).

supplemental brief contains little if any discussion of statutory interpretation. It follows that the Court should resolve this dispute by reference to the plain language of the Election Code.

Second, assuming there were an ambiguity here, deference to an agency's interpretation of a statute is the eighth of eight enumerated factors that a court ***may*** consider. *See* 1 Pa. Cons. Stat. Ann. § 1921(c)(8). Other factors include the "circumstances under which it was enacted" and the "contemporaneous legislative history." *Id.* § 1921(c)(2), (c)(7). This makes sense, as "[t]he object of all interpretation and construction of statutes is to ascertain and effectuate ***the intention of the General Assembly***." *Id.* § 1921(a) (emphasis added); *see also Chem. Mfrs. Ass'n v. Natural Res. Def. Council, Inc.*, 470 U.S. 116, 126 (1985) (finding that court should not defer to agency's interpretation if "the legislative history or the purpose and structure of the statute clearly reveal a contrary intent").[16] Here, Petitioners' reading of the Election Code is irreconcilably inconsistent with the legislative history. *See infra.* It follows that deference to a contrary reading would be inappropriate.

Third, this is not a case where an agency is interpreting its own regulations, interpreting its enabling statute, or even interpreting a statute it has exclusive authority to implement. Indeed, Respondent has recently argued (in another context) that her office lacks substantial experience with electronic voting,[17] and when not asking for this Court's deference she has gone out of her way to deemphasize responsibility for implementing or ensuring compliance with the law. *See,*

---

16 Respondent's authority is not to the contrary. She relies heavily on *Dechert LLP v. Com.*, 606 Pa. 334, 350, 998 A.2d 575, 585 (2010). In that decision, while Chief Justice Castille did note that his reading of the statute at issue is consistent with the agency's reading, he did so only after satisfying himself that his reading was consistent with the legislative history. *See id.* at 350, 998 A.2d at 585. It is apparent from his opinion that he would not defer to an agency's interpretation that was at odds with the legislative history. *See id.*

17 *See* Resp't's Opp'n to Mot. to Compel dated Apr. 1, 2013, ¶ 30 ("Mr. Cobb was hired because the Commonwealth lacks the internal resources and/or adequate prior experience within Mr. Cobb's field."); *id.* ¶ 41 ("[Mr. Cobb] was, instead, retained by the Secretary, whose office lacked 'sufficient internal resources' or experience in voting-system technology....").

e.g., Resp't's Supp. Br. at 27 (discussing Respondent's "limited role" in testing EVSs). Unlike an agency that has exclusive authority to implement a statute, Respondent concedes —indeed, insists—that she at most has coordinate responsibilities with many other officials. It follows that her reading is not entitled to deference.[18]

Finally, courts do not defer to "interpretations" that agencies develop during litigation. *See Bowen v. Georgetown Univ. Hosp.*, 488 U.S. 204, 212-13 (1988) ("[W]e have declined to give deference to an agency counsel's interpretation of a statute where the agency itself has articulated no position on the question . . . . Deference to what appears to be nothing more than an agency's convenient litigating position would be entirely inappropriate."); *see also St. Elizabeth's Child Care Ctr.*, 600 Pa. at 142, 963 A.2d at 1280 (Baer, J., concurring) ("I am bothered generally by administrative bodies citing their own interpretations in blind support of positions they advocate in litigation."). Not surprisingly, the decisions Respondent has cited involved interpretations that were settled before litigation began. *See, e.g.*, *id.* at 135-36, 963 A.2d at 1276 (agency's interpretation held for more than 30 years prior to litigation); *see also Dechert LLP*, 606 Pa. at 350, 998 A.2d at 585 (Department of Revenue published its interpretation more than three years before litigation); *Kuznik v. Westmoreland Cnty. Bd. of Comm'rs*, 588 Pa. 95, 108, 902 A.2d 476, 483 (2006) (agency's interpretation announced more than two years before litigation commenced); *Nationwide Mut. Ins. Co. v. Foster*, 143 Pa. Cmwlth. 433, 436, 599 A.2d 267, 269 (1991) (litigation commenced after Insurance

[18] Respondent cites *St. Elizabeth's Child Care Ctr. v. Dep't of Pub. Welfare*, 600 Pa. 131, 963 A.2d 1274 (2009) in support of this argument. In that case, however, the court deferred to an agency's interpretation of its own enabling statute during the course of a formal adjudication, neither of which applies here. *See id.* at 136, 963 A.2d at 1276. She has also cited that decision in reading something into the lack of remedial legislation. That is hard to reconcile, however, with the fact that DREs were not widely used in the Commonwealth until 2006, at which point these issues were submitted to this Court. *See, e.g.*, Memorandum from W. Boehm to D. Cooper dated Dec. 14, 2006 (Ex. 31) at 7.

Commissioner published and interpreted the "Statement of Policy"). Here, Respondent points to nothing in the record that shows that she or her predecessor engaged in a thoughtful analysis of phrases such as "preclude every person from tampering with the tabulating element" before this litigation commenced. Absent such evidence, deferring to her litigation positions would be wholly improper.

B. Respondent's Factual Arguments Find No Support In The Facts

Petitioners claim that Respondent certified DREs that do not preclude tampering with "tabulating elements" or "ballots" as required by the Election Code (Count II), that she did not reexamine DREs in a way that ensured compliance with the Election Code (Counts III and VII), and that she certified DREs in violation of the Pennsylvania Constitution (Counts VII, IX & X). As to each claim, material facts are in dispute.

1. There Is A Genuine Issue Concerning Whether DREs "Preclude" "Every Person" From Tampering with "Tabulating Elements"(Count II)

a. Whether DRE Tabulation Element Tampering Has In Fact Occurred In Pennsylvania Or Elsewhere Is Not A Material Fact

Respondent asks the Court to enter summary judgment in her favor because she believes there is no evidence that DRE tampering has happened in an actual election in Pennsylvania. She repeats this shibboleth throughout her brief. *See* Resp't's Supp. Br. at 3, 22, 28, 29, 30, 31, 40, 41, 42, 53, 54, 55 and 58.

As an initial matter, even if we assume that there is no evidence of tabulation tampering, it does not necessarily follow that it has not happened. On the contrary, it is entirely possible that tabulation tampering has occurred and has not been detected. Indeed, Respondent's expert once acknowledged as much:

> Computerized 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.

Ronnie Dugger, *Annals of Democracy – Counting Votes*, The New Yorker (Nov. 7, 1988) (Ex. 5) at P-15195 (quoting Dr. Shamos); *see also* Hearing Before The Texas House Committee on Elections (Nov. 25, 1986) (Ex. 16) at P-15740-42 (discussing punch card systems) ("Once the evidence is removed from the voting booth there's just simply no way of proving that there's ever been any tampering. You certainly – you can count and recount and count the votes 50 times and you'll get the same totals. They'll just be wrong because the voter's intentions were frustrated."). One of Petitioners' experts testified to that effect as well. *See, e.g.*, Lopresti 2011 Report (Ex. 18) at 9 ("It is also wrong to believe that such tampering is always detectable after-the-fact. As I have previously noted, most types of electronic computer memory used in DREs are freely rewriteable. Since memory can contain both data (votes) and program code, malicious software has the ability to alter not only electronic voting records (including audit logs), it can also effectively 'erase' itself after it has done its job.").

Even so, the material fact is not whether tabulation tampering ***has*** happened, but whether it ***could*** happen. The materiality of this fact flows from the Election Code itself, which requires that all EVSs "shall preclude" "every person" from "tampering with the tabulating element."[19] That language is perfectly clear; "shall" is obligatory and "preclude" and "every person" are absolute. Respondent argues that the Election Code cannot require that tampering be made

---

[19] *See* Section 1107-A(17)(i), 25 Pa. Stat. Ann. § 3031.7(17)(i) ("If the voting system is of a type which provides for the computation and tabulation of all votes at a central counting center or if it provides for the tabulation of district totals at such a central counting center, the central automatic tabulating element shall include the following mechanisms or capabilities: (i) ***It shall be constructed so that every person is precluded from tampering with the tabulating element during the course of its operation***") (emphasis added); Section 1107-A(16)(iii), 25 Pa. Stat. Ann. § 3031.7(16)(iii) ("If the voting system is of a type which provides for the computation and tabulation of cotes at the district level, the district component of the automatic tabulating equipment shall include the following mechanisms or capabilities: (iii) …; ***and it shall preclude every person from tampering with the tabulating element.***") (emphasis added).

impossible because no computer is perfect. *See, e.g.*, Resp't's Supp. Br. at 42 ("The laws of physics ... dictate that such a standard is impossible to meet and, therefore, is not applicable...."). Notably, Respondent cites her expert's reports in support of that argument but fails to cite his more candid (and polar opposite) views from before this litigation began:

> The [Election Code] is phrased in very superlative terms. It says the system must be capable of absolute accuracy in counting – in counting up the results of an election. ***I believe that absolute accuracy means it must get the vote totals correct to zero – zero error tolerance. Not one vote can be counted incorrectly.*** That's a very high standard. It's so high that it's virtually impossible for any system to meet it, therefore ***the vendor claims that it shouldn't be held to that standard. So what good is it if we have legislation if the – those who would be regulated argue that the legislation is inapplicable?***

(Ex. 16) at P-15753-54 (quoting Dr. Shamos) (emphasis added). Respondent also fails to cite this Court ruling on her preliminary objections, which rejected a similar argument.[20]

In Respondent's view, it is up to her to decide what degree of security vulnerability is and is not acceptable. *See* Resp't's Supp. Br. at 42-43. These provisions say nothing of the sort, however. And as Respondent herself acknowledges elsewhere in her brief, it is "the General Assembly, and not the courts of Pennsylvania or the executive branch, [that] is responsible for setting election law and policy in the first instance." *Id.* at 45; *see also id.* at 46 (noting the "General Assembly's constitutional prerogative to make laws relating to the election process"); *id.* at 2 ("[I]t is the General Assembly that is responsible for identifying what is truly necessary for the conduct of safe and efficient elections."). Petitioners agree with that. As noted above, the legislature refused to allow EVSs to be used in elections without a number of safeguards,

---

[20] *See Banfield I*, 922 A.2d at 48 ("The Secretary also asserts that no voting system is perfect and that the possibility of malfunction does not constitute an equal protection violation. However, Electors allege that, unlike any other voting system, the challenged DREs have no meaningful recount or audit mechanisms when they malfunction.").

one of which that EVSs preclude every person from tampering with tabulation. It is not for Respondent or even this Court to second guess that judgment.

That is especially true here because other provisions at least arguably give Respondent some degree of discretion to determine what is and is not "acceptable." Specifically, whereas the provisions concerning "tabulation element" security speak in absolute terms, the provision concerning "ballot" security speaks in terms of what is "acceptable." *Compare* 25 Pa. Stat. Ann. § 3031.7(17)(i) *and* 25 Pa. Stat. Ann. § 3031.7(16)(iii) *with* 25 Pa. Stat. Ann. § 3031.7(12). The parties disagree about what the phrase "acceptable ... to prevent tampering" means, *see infra*, but there can be no disagreement about whether the phrase applies here. Nor can there be disagreement that the General Assembly knew how to afford some degree of discretion when it wanted to and decided not to do so here. *See, e.g.*, *Fonner v. Shandon, Inc.*, 555 Pa. 370, 378-79, 724 A.2d 903, 907 (1999) ("[W]here the legislature includes specific language in one section of the statute and excludes it from another, the language should not be implied where excluded."). It follows that the material fact is whether any person can tamper with the DREs' tabulating elements – not how likely it is, and certainly not whether Respondent deems that likelihood acceptable or not.

b. There Is A Genuine Issue Regarding Whether DREs "Preclude" "Every Person" From Tampering With The "Tabulating Element"

There are many ways to tamper with a DRE's tabulating element in order to alter a vote. 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. *See, e.g.*, Jones 2011 Report (Ex. 23) ¶ 95("[T]he key security vulnerabilities required to permit construction of a virus are present."). Similarly, the Halderman Report concluded that the Diebold AccuVote-TS was susceptible to tabulation tampering:

- ***Malicious software running on a single voting machine can steal votes with little risk of detection***. The malicious software can modify all of the records, audit logs, and counters kept by the voting machine, so that even careful forensic examination of these records will find nothing amiss. ***We have constructed demonstration software that carries out this vote-stealing attack***;

- ***Anyone who has physical access to a voting machine, or to a memory card that will later be inserted into a machine, can install said malicious software using a simple method that takes as little as one minute***. In practice, poll workers and others often have unsupervised access to the machines;

- AccuVote-TS machines are susceptible to voting-machine viruses – computer viruses that can spread malicious software automatically and invisibly from machine to machine during normal pre and post-election activity. ***We have constructed a demonstration virus that spreads in this way, installing our demonstration vote-stealing program on every machine it infects.***

The Halderman Report (Ex. 15) at 2 (emphasis added); *see also* Brennan Report (Ex. 14) at 13966 (identifying over 35 potential attacks against DREs; "[a]ll of the least difficult attacks against DREs without VVPAT involve inserting Software Attack Programs into the DREs.").

Moreover, 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. *See* 2008 Jones Report (Ex. 22) ¶ 36. He explained: "[i]n spite of the proprietary nature of the 'official' PEB it was relatively simple to emulate a PEB to an iVotronic or to read or alter the contents of a PEB using only inexpensive and commercially available IrDA-based computing devices (such as a Palm Pilot PDAs and various mobile telephones)." *Id.* As a result both the firmware and the configuration of the ES&S precinct hardware can be "easily tampered with in the field." *Id.* Specifically, "[v]irtually every piece of critical data at a precinct – including precinct vote tallies, equipment configuration and equipment firmware – can be compromised through exposed interfaces, without knowledge of passwords and without the use of any

specialized proprietary hardware." *Id.* Similarly, on a different machine, an attacker with physical access to the inside of the machine's case "could … compute the System Key from the serial number than use it to decrypt the other keys." *Id.* at 35. "Or, the smart card authentication protocol can be broken" and "[s]ecurity key cards can be forged and used to change system keys." *Id.* (referencing vulnerability identified in California Top to Bottom Report) (quotations omitted).

Respondent does not even try to deny that, if successful, these attacks would alter votes. Indeed, her counsel admitted as much at oral argument,[21] and her expert admitted as much at deposition.[22] Instead, Respondent suggests that locks and seals on tabulating elements is an adequate safeguard. *See, e.g.*, Resp't's Supp. Br. at 23. But that too is genuinely in dispute.

Respondent's reliance on locks and seals also ignores a large body of research showing that locks and seals can be bypassed easily and undetectably. For example, Dr. Appel and others at Princeton University authored a report detailing insecurities associated with the Sequoia AVC Advantage. *See* Insecurities and Inaccuracies of the Sequoia AVC Advantage 9.00H DRE Voting Machine, Oct. 17, 2008 (attached hereto as Ex. 27). An entire section of the report is dedicated to the DRE's locks, which the report concluded were "simple, cheap and easy to pick" in a matter of "seconds." *Id.* at P-12779-12782. As for the machine's seals, the report concluded

---

21 *See* Recording of Oral Argument dated Nov. 16, 2011 ("J. Cohn Jubilerer: Would it be possible to program the software inside the machine so that – Mr. Bizar: It has never been done. J. Cohn Jubilerer: It hasn't been done but – Mr. Bizar: It has never been done. J. Cohn Jubilerer: but is it possible that somebody … would be able to program these machines so that it would change the votes and then sort of destroy itself – Mr. Bizar: Undoubtedly …it's possible to do that. There are creative people who can do these kinds of things. They can also stuff ballot boxes with paper ballots or alter ballots with additional marks. And they can – there are millions of different ways….") (official transcription unavailable).

22 *See* Shamos Dep. at 181-82 (Ex. 9); *see also id.* at 92.

that they afforded no real protection because the circuit board could be removed without removing the seal. *Id.* at P-12782-12789.

Similarly, the California Top to Bottom Review concluded that locks on the Sequoia AVC Edge can be bypassed by unscrewing screws, and reported that the screws were not covered with seals. *See* Ex. 19 at P-09955-09966. That study also shows that plastic covers "protected by seals" could by pried open so that tools could manipulate the protected buttons without damaging the seals or leaving evidence that the security of the system had been compromised. *See id.*

Rather than deny that tampering is possible, Respondent argues that tampering would be prevented or uncovered in "real world elections" as opposed to "the academic environment of a classroom or lab." Resp't's Supp. Br. at 25-26, 29; *see also* Shamos Report (attached as Ex. 7 to Resp't's Supp. Br.) ¶¶ 188, 232, 276, 368, 470. To the extent Respondent is arguing that the Election Code is only concerned about vulnerabilities that someone has actually already exploited in a live election, she is plainly wrong. And to the extent Respondent is arguing that Sections 3031.7(17)(i) and 3031.7(16)(iii) account for procedural safeguards other than those in the DREs themselves, she is wrong about that too. Those provisions require that EVS "automatic tabulating equipment" precludes tampering, not that poll workers do so. They do not allow Respondent to certify EVSs with insecure tabulating equipment simply because she hopes "administrative and procedural protections" might deter fraud. Resp't's Supp. Br. at 26; *see also, e.g.*, Jones 2011 Report (Ex. 23) ¶ 93 ("Dr. Shamos does not dispute that the iVotronic PEB attack allows a person to tamper with an iVotronic" and "to do anything that can be done with a PEB, including voting more than once. I do not see an escape clause here permitting polling procedures to substitute for the mechanism.").

But even if that were material, that is genuinely disputed as well because Petitioners' experts have concluded that these security vulnerabilities ***could*** be exploited in a live election. For example, 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." Jones 2008 Report (Ex. 22) ¶ 40; *see also id.* ¶ 57 ("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 involves violation of the voter's right to privacy in the voting booth."). Similarly, Dr. Lopresti testified at deposition that it was possible that these security vulnerabilities "could actually happen in Pennsylvania in an election." Lopresti Dep. Tr. (attached hereto as Ex. 28) at 237. This difference of opinion among the parties' experts creates a question of credibility that requires a trial. *See supra* Section II.A.

2. There Is A Genuine Issue Concerning Whether DREs Have "Acceptable Ballot Security" To "Prevent Tampering" With "Ballots" (Count II)

Count II also asserts that the DREs do not comply with Section 3031.7(12) of the Election Code, which requires that EVSs "provide acceptable ballot security procedures . . . to prevent tampering with or substitution of any ballots."[23] As with the tabulation tampering claim, this ballot tampering claim raises genuine issues of material fact.

There is evidence that DRE ballots can be tampered with both easily and undetectably.[24] For example, Dr. Lopresti noted that the California Top to Bottom Review revealed "an attack in

---

[23] 25 Pa. Stat. Ann. § 3031.7(12). The Election Code defines "ballot" as "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***...." 25 Pa. Stat. Ann. § 3031.1 (emphasis added).

[24] *See, e.g.,* Candice Hoke, *Chapter 17: Voting Technology and the Quest for Trustworthy Elections, in America Votes! A Guide to Modern Election Law & Voting*, Section I: Background:

(Continued)

which a voter, using a few easily concealed tools, can reset the [Diebold] TSx DRE to administrative mode, delete all ballots cast thus far on the machine, and restart the election on the unit." Lopresti 2008 Report (Ex. 24) ¶ 17(b)(i). Additionally, Dr. Jones explained how memory cards could be used to tamper with ballots: "[w]hen a memory device the size of a large postage stamp or a pack of cigarettes is involved, as is the case with current DRE voting systems, it is vulnerable to sleight of hand manipulations. As a result, unlike conventional ballot boxes, it is almost impossible for an observer to see that the memory card inserted in the envelope for transport to the county buildings is indeed the one that was pulled from the machine only seconds earlier." Jones 2008 Report (Ex. 22) ¶ 51. The California and Ohio reports list other viable attack scenarios. *See* Excerpts from California Top to Bottom Review (Ex. 19) at P-09931-09937 (Diebold Accuvote TSx); *id.* at P-09952 (Hart InterCivic); *id.* at P-09963-09965 (Sequoia AVC Edge); *see also* Excerpts from Ohio EVEREST Report (Ex. 20) at p-13377-13379 and p. 93-99 (ES&S iVotronic attack scenarios) available at http://www.patrickmcdaniel.org/pubs/everest.pdf; *id.* at 191-194 (Accuvote TSx); *id.* at 267-270 (Hart Intercivic). Finally, the "Man in the Middle" attack described by the Argonne National

---

(Continued)

Performance Records of E-Voting Systems, at n.22 (Benjamin E. Griffith, 2nd ed. 2012), available on Westlaw at ABA-AMVOTE § 17.1 ("A DRE is a direct recording electronic voting unit that digitally records voters' choices. . . . Independent testing has shown that these all-electronic units can be made to 'cheat' – either deliberately by human tampering or inadvertently because of buggy software or other defects.") (citations omitted); *id.* at § 17.1, Section II: Federal Compulsion to Adopt Software-Based Voting Technologies ("[T]ampering may be completely undetectable, leaving observers and participants believing that the machines . . . are functioning accurately and neutrally.").

Laboratory is another example of a threat that can be carried out during the course of a live election with a few minutes and a few dollars worth of equipment. *See supra.*

Respondent does not meaningfully engage this evidence. Instead, she simply notes that "a review is made to determine whether there are security vulnerabilities that could feasibly be exploited" and "a check is made to determine the degree to which the system resists attempts to alter its records." Shamos Report (attached as Ex. 7 to Resp't's Supp. Br.) ¶ 64. It is clear, then, that Respondent is hanging her hat on the presence of the word "acceptable" in Section 3031.7(12), the implication being that it gives her unfettered discretion to determine how much security – if any – will pass muster.

There are at least three flaws in this argument. The first and most important is that she and her current examiner did not conduct "a review...to determine whether there are security vulnerabilities," which would be necessary to even begin to determine that these vulnerabilities "could feasibly be exploited." Consequently, any exercise of discretion as to what is acceptable is arbitrary because it does not attempt to decide on the basis of a reasonable review of all the evidence but on the basis of a deliberately limited set of facts. *See infra.*

The second flaw is that Respondent's reading of "acceptable" ignores the language and history of the statute. Respondent focuses on "acceptable" to the exclusion of "prevent" and the legislative history that the General Assembly wanted security and integrity in the voting process. The more natural reading of the statute, and the one that is consistent with its legislative history, is that respondent has discretion to weigh unknown possibilities but not known vulnerabilities. Otherwise Respondent would be free to substitute her preferences (preventing some tampering) for those of the General Assembly (preventing all tampering).

To be sure, new and unexpected methods for hacking into computers will always arise. EVSs need not prevent exploits that are not yet known to science, and the Secretary need not withhold certification because someone somewhere might someday develop something new. That may well be an impossible standard to satisfy. *Cf.* Resp't's Supp. Br. at 43 ("One may pronounce a system 'secure' against a given set of threats, ***but not against threats that have not yet been invented or articulated***.... [T]here will never be a certification ... that can guarantee that no intruder will ***ever*** be able to subvert that system.") (emphasis added). But that does not mean it is "acceptable" to tolerate vulnerabilities that are not only well documented in scientific literature but have also been demonstrated in simulated election conditions, or that the Secretary can grant certification because she believes such a vulnerability is unlikely to be exploited in a "real election." Responsible government entities and commercial enterprises take reasonable steps to respond to new security threats as they arise. According to Respondent's own expert, that would not be an impossible standard to satisfy. *See, e.g.*, Hearing before the Committee on House Administration, Hearing On Verification, Security And Paper Records For Our Nation's Electronic Voting Systems (Sept. 28, 2006) (Ex. 26) at P-15336 ("Professor Felten at Princeton, Harri Hursti, and others have done a great service by exposing security vulnerabilities in voting systems. Some of these vulnerabilities are severe and require immediate repair, ***but the point is that they are easily remedied***.") (quoting Dr. Shamos) (emphasis added). In any event, that is precisely the standard the General Assembly imposed. *See* 25 Pa. Stat. Ann. § 3031.5(c) ("[I]f, upon the reexamination of any such system previously approved, it shall appear that the system so reexamined can no longer be used safely by voters at elections as provided in this act or does not meet the requirements hereinafter set forth, the approval of that system shall forthwith be revoked...."); *see also* Hearing before the Environment, Technology & Standards Subcommittee

of the Committee on Science, U.S. House of Representatives, Testimony of Michael I. Shamos (June 24, 2004) (Ex. 11) at 3 ("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. But the glacial pace of prior development of voting standards is no longer acceptable to the public.").

The third flaw is that Respondent has exercised whatever discretion she has based on a fundamentally flawed premise: that pre-election testing will ensure the security of the system and the integrity of voting. That particular procedural safeguard will do nothing at all to detect, much less prevent, any tampering that occurs during the course of an election. It is for that reasons that, as one commentator observed, "[i]f you wanted to know where the next great eruption of voting-machine scandal is likely to emerge, you'd have to drive deep into the middle of Pennsylvania." Clive Thompson, New York Times, *Can You Count on Voting Machines?* (June 6, 2008) (attached hereto as Ex. 29). He recounted the following experience before an election:

> On the Friday before the November elections in Pennsylvania, I wandered into a church in a suburb of Pittsburgh. The church was going to serve as a poll location, and I was wondering: Had the voting machines been dropped off? Were they lying around unguarded — and could anyone gain access to them?
>
> When I approached the side door of the church at 6 p.m., two women were unloading food into the basement kitchen. (They were visitors from another church who had a key to get in, but they told me they'd found the door unlocked.) I held the door for them, chatted politely, then strolled into the otherwise completely empty building. Neither woman asked why I was there.
>
> I looked over in the corner and there they were: six iVotronic voting machines, stacked up neatly. While the women busied themselves in their car, I was left completely alone with the machines. The iVotronics had been sealed shut with numbered tamper seals to prevent anyone from opening a machine illicitly, but cutting and resealing them looked pretty easy. In essence, I could have tampered with the machines in any way I wanted, with very little chance of being detected or caught.

> Is it possible that someone could hack voting machines and rig an election? Elections officials insist that they are extremely careful to train poll workers to recognize signs of machines that had been tampered with. They also claim, frequently, that the machines are carefully watched. Neither is entirely true. Machines often sit for days before elections in churches, and while churches may be wonderfully convenient polling locations, they're about as insecure a location as you could imagine: strangers are *supposed* to wander into churches.

Id.

Petitioners' experts agree that pre-election testing is not an adequate safeguard. *See, e.g.*, 2011 Jones Report at ¶ 93 (Ex. 23); 2008 Jones Report at ¶ 57 (Ex. 22). Indeed, even Respondent's own expert once noted the folly of relying on pre-election testing:

> [W]e don't have any real security. The reason for that is it's possible for a programmer to arrange software so that it counts the ballots absolutely correctly at all times except on election night when it substitutes its own will for that of the voters. The reason it can do that is that I can go in during – during the election and submit a special card instead of my ballot. I'll sacrifice one vote in order to fix the election. Instead of putting in the ballot card, I'll put in a special card that the program has been modified to wait for. When it sees that card it says, aha, must be election night, and so I'll put in the pre-stored results for the outcome of the election that I would like determined. And then no matter how many times a recount is done, as long as that card is in there it will tell the system, aha, it's election night or they're doing a recount and the predetermined fixed results will be done. Yet if anybody goes to the system, doesn't have that card in there and tries to do a test, they will only get the exact correct results. ***So the fact that a system works on small tests or even tests done months before the election does not give me great confidence that nothing is going on funny on election night.***

Tr. of Hearing Before the Texas House Committee on Elections (Nov. 25, 1986) (Ex. 16) at P-15755-57 (emphasis added). Dr. Shamos was discussing earlier generation machines to be sure, but his logic still holds.

In short, it is Respondent, not Petitioners, who is trying to subvert the legislative process. Respondent may well think that her interpretation of Section is sound policy for some reason. But as she herself acknowledged, it is "the General Assembly, and not the courts of Pennsylvania or the executive branch, [that] is responsible for setting election law and policy in the first

instance." Resp't's Supp. Br. at 45; *id.* at 46 (noting the "General Assembly's constitutional prerogative to make laws relating to the election process"). To the extent Respondent is acting upon a faulty premise, her actions are not entitled to any degree of deference.

3. There Is A Genuine Issue of Material Fact Concerning Whether Respondent Uses Testing Procedures That Ensure DREs Comply With the Election Code (Counts III & VII)

An *en banc* panel of this Court previously found that Respondent was obliged to test EVSs for compliance with every requirement of the Election Code. At a minimum, there is a genuine issue of material fact concerning whether her recent reexaminations did so, particularly with regard to the security requirements discussed above. *See* 25 Pa. Stat. Ann. § 3031.7(12) (ballot security); *id.* at §§ 3031.7(17)(i), 3031.7(16)(iii) (tabulating element security).

a. The Election Code Requires Security Testing, Not Blind Reliance on Out Of Date ITA Reports That Were Not Even Reliable When Made

Although she characterizes her reexaminations as "detailed and rigorous," Resp't's Supp. Br. at 13, it is telling that Respondent's primary defense of those reexaminations is her belief that security testing was not necessary in the first place. *See id.* at 24.[25] Specifically, she cites her expert for the proposition that the Election Code "expressly delegates the 'testing' function not to the Secretary but to an independent testing authority." *Id.* In other words, she believes that the only material fact insofar as this claim is concerned is whether an ITA examination occurred.

If Respondent believes that, she is operating under a mistaken view of the Election Code and there is no doubt that this Court can compel compliance with it. Although Section 3031.5 does require that an ITA conduct an examination for compliance with ***federal law***, that is simply

---

[25] She also argues that she "cannot … test individually each of the thousands of DRE machines that are actually used" in elections. *Id.* at 27. That is a straw man; Petitioners have never suggested that she should or even could have done that. Petitioners have only asked that she examine each system. But it seems she is unwilling to do even that in any responsible way.

a precondition for a vendor's asking Respondent to conduct her own separate examination for compliance with ***Pennsylvania law***.[26] Nothing in the Election Code relieves Respondent from her obligation to test for compliance with Pennsylvania law.[27] Indeed, the very next paragraph of Section 3031.5 confirms that she must test for compliance with "***all of the requirements hereinafter set forth***,"[28] which includes the requirements of Sections 3031.7(12), 3031.7(17)(i) and 3031.7(16)(iii). So, for that matter, did this Court.[29] Respondent's reading of the statute is untenable because it would render whole swaths of the Election Code a nullity,[30] and, as her own expert put it before litigation commenced, would allow her to "abdicate" her official duties.[31]

---

[26] *See* 25 Pa. Stat. Ann. § 3031.5(a) ("Any person or corporation owning, manufacturing or selling ... any electronic voting system, may request the Secretary of the Commonwealth to examine such system if the voting system has been examined and approved by a federally recognized independent testing authority and if it meets any voting system performance and test standards established by the Federal Government.").

[27] Nor does anything in HAVA purport to preempt states from conducting examinations to ensure compliance with state law requirements that are consistent with it. On the contrary, HAVA's savings clause expressly preserves states' right to do so. *See* 42 U.S.C. § 15484 ("**MINIMUM REQUIREMENTS.** The requirements established by this title are minimum requirements and nothing in this title shall be construed to prevent a State from establishing election technology and administration requirements that are more strict than the requirements established under this title so long as such State requirements are not inconsistent with the Federal requirements under this title or any law described in section 906.").

[28] *See* 25 Pa. Stat. Ann. § 3031.5(b) ("[T]he Secretary of the Commonwealth shall examine the electronic voting system and shall make and file in his office his report, attested by his signature and the seal of his office, stating whether, in his opinion, the system so examined can be safely used by voters at elections as provided in this act and meets ***all of the requirements hereinafter set forth.***") (emphasis added).

[29] *See Banfield I*, 922 A.2d at 42-43 ("To the extent that the Secretary believes that section 1105-A allows the Secretary to examine DREs without regard to the requirements of the Election Code, the Secretary is mistaken.").

[30] *See, e.g.*, *Masland v. Bachman*, 473 Pa. 280, 291 (1977) ("This is contrary to principle (sic) that the Legislature is not presumed to have intended the provisions of its enactments as mere surplusage."); *In re Sale of Real Estate by Lackawanna Co. Tax Claim Bureau*, 22 A.3d 308, 316 (Pa. Commw. Ct. 2011) ("Section 1922 of the Statutory Construction Act . . . 'prohibits courts from interpreting statutes in a way that makes words used in statutes meaningless or mere surplusage.'") (citation omitted).

[31] *See* Hearing before the Environment, Technology & Standards Subcommittee of the Committee on Science, U.S. House of Representatives, Testimony of Michael I. Shamos (June 24, 2004) (Ex. 11) at 1 ("Many states that formerly had statutory certification procedures have

(Continued)

Respondent's abdication is particularly troubling because there is general agreement that the ITA process is inadequate. Petitioners' expert was highly critical of testing conducted by ITAs: "I have encountered numerous cases where ITA testing has clearly been deficient." 2011 Jones Report (Ex. 23) ¶ 69. He opined that it is "irresponsible ... for a state to rely on ITA or VSTL testing without assessing the adequacy of those tests and determining if any requirements have not, in fact, been tested." *Id.* at ¶ 68; *id.* at ¶ 77 ("I have seen no evidence of anything approaching a design review in any of the work done by the ITAs or by the Commonwealth...."). If anything, Respondent's expert was even more critical, calling the ITA examination process at that time "dysfunctional," "virtually non-existent," "not effective" and "[in]adequate." *See supra* Section III.C. Respondent's expert defended her reliance on ITAs by citing the costs of conducting her own examinations, not the quality of the ITA's examinations.

b. Even If ITA Testing Were Reliable, It Is Arbitrary And Capricious To Rely On Tests That Predate The Discovery of New Vulnerabilities

It is one thing to rely on the report of a third party who actually purported to do testing. It is quite another to rely on the report of a third party who did not. Respondent's reliance on ITAs during the course of her recent reexaminations is the latter.

In conducting the recent reexaminations, Mr. Cobb relied almost entirely on ITA reports. For example, Section 4.1 of each of the re-examination reports is titled "Review" and identifies four subsections of the Election Code for which ITA reports were referenced as the sole basis of information upon which compliance was determined. *See, e.g.,* Ex. 13 to Resp't's Supp. Br. at 5 (Sequoia AVC Edge Re-examination Report). Thus, ITA reports were the basis of his

---

(Continued)

abdicated them in favor of requiring no more from a vendor than an ITA qualification letter.... My own state, Pennsylvania, abandoned certification in 2002 because it believed the ITA process was sufficient. We are less safe in 2004 than we were 20 years ago.").

conclusion that DREs satisfied Section § 3031.5(a) (requiring ITA approval); § 3031.7(11) ("suitable design" and "capable of absolute accuracy"), Section 3031.7(13) (requiring a DRE "[w]hen properly operated, records correctly and computes and tabulates accurately every valid vote registered"), Section 3031.7(14) (requiring DREs be safely transportable), and Section 3031.7(15) (requiring that DREs be "so constructed that a voter may readily learn the method of operating it.").

That is especially troubling when one considers that Respondent and Mr. Cobb were relying on ITA reports that predated the large body of scientific knowledge regarding DRE security vulnerabilities. *See* Ex. 9 to Resp't's Supp. Br. (Danaher Controls, Inc. Electronic 1242 Voting System), Test Protocol at 6 (referencing ITA reports dated March and April 2005); Ex. 10 to Resp't's Supp. Br. (Accuvote TSx Voting System), Test Protocol at 4 (referencing ITA reports dated July 2005 and November 2005 and Software ITA report dated March 2007); Ex. 11 to Resp't's Supp. Br. (iVotronic Touch Screen Voting System), Test Protocol at 6 (referencing ITA reports dated October 2005 and March 2006); Ex. 12 to Resp't's Supp. Br. (Hart Voting System 6.2.1), Test Protocol at 6 (referencing ITA reports dated August 2006); Ex. 13 to Resp't's Supp. Br. (Dominion AVC Edge Model 2), Test Protocol at 5 (referencing ITA reports from March 2006); Ex. 14 to Resp't's Supp. Br. (Sequoia AVC Advantage 10), Test Protocol at 5 (referencing ITA reports from September and October 2006); *see also, e.g.*, Jones 2011 Report (Ex. 23) ¶ 70 ("All of the voting system certifications that are the subject of this case were produced by that flawed [pre-2007 ITA] system"). In other words, they relied on reports from 2005 and 2006 in deciding that DREs precluded tampering in 2012 – this despite authoritative work from the Top to Bottom Review, the EVEREST Report, the Brennan Center Report, the

Halderman Report, the Florida SAIT Report and the Argonne National Laboratory that was to the contrary.

Respondent has said that her office originally declined the requests for reexamination for the "prudential reason that the requesting electors had not identified any reason why reexaminations of the systems would produce a result different from the examinations" that had just been done. Resp't's Resp. to Mot. to Compel ¶ 4 (April 1, 2013). It would stand to reason, then, that the reexaminations she conducted many years later would take into account the mounting security vulnerabilities that had been revealed in the meantime. She did no such thing. On the contrary, her re-examiner relied on outdated ITA reports and did not even attempt to replicate any of the attacks identified in the literature that was published in the following years. *See* Cobb Dep. Tr. (attached hereto as Ex. 30) at 130 ("My knowledge of the California Top-to-Bottom review is not extensive enough to – to do a comparison with the exact stuff in the test report); *Id.* at 131 (stating did not consider the Ohio Everest Report in re-examinations). In fact, he had not even heard of the Man in the Middle attack that was developed by the Argonne National Laboratories. *Id.* at 137-38. Or the Halderman report analyzing the vulnerabilities in the Diebold. *Id.* at 132. Or the Florida SAIT report. *Id.* Or the Appel report on the Sequoia Advantage. *Id.* at 205.

c. Mr. Cobb's Purported "Penetration Analysis" Was So Superficial That It Did Not Satisfy The Election Code In Any Meaningful Way

Section 4.4 of all of Mr. Cobb's re-examination reports is titled "Penetration Analysis" and details the analysis that Mr. Cobb conducted to test for compliance with Section 3031.7(12). A comparison among all the re-examination reports shows that the summary of the penetration analysis for each machine was almost identical. *Compare* Ex. 9 to Resp't's Supp. Br. at § 4.4 p. 12 *with* Ex. 10 to Resp't's Supp. Br. at § 4.4 p. 12 *and* Ex. 11 to Resp't's Supp. Br. at § 4.4 p. 11

and Ex. 12 to Resp't's Supp. Br. at § 4.4 p. 12 *and* Ex. 13 to Resp't's Supp. Br. at § 4.4 p. 10 *and* Ex. 14 to Resp't's Supp. Br. at § 4.4 p. 11. When asked about the specific components of the Penetration Analysis, Mr. Cobb explained his testing:

> Check that all seals, locks, attempts to open the system. Verify the ballot storage device is secure by attempting to insert and retrieve ballots without removing any seals and/or locks. Verify that the needed supplies can be accessed by the poll worker without allowing access to the ballots or internal components of the voting system. Verify that the system counter cannot be reset by an unauthorized person at any unauthorized point. Exercise verification of password security management.

Cobb. Dep. Tr. (Ex. 30) at 124. When asked if anything else was involved in his penetration analysis, he said "no." *Id.* at 124-25. When asked how the he tested locks and seals, Mr. Cobb replied: "We examined the locks to make sure they were in place, we examined the seals to make sure they were secure." *Id.* at 169. He did not, however, attempt to break a seal and reassemble it. *Id.* at 169-70. Mr. Cobb was asked: "How was it determined whether tampering in a case was or was not evident based on your examination? A. During the exam, we observed the locks and seals that were in place. To what degree that showed evidence is they were still there, they were in place." *Id.* He did not recall how much time was spent analyzing the locks and seals. *Id.* He did not consult outside sources to determine fruitful ways to tamper with locks or seals without evidence. *Id.* And he did not consider attempts to bypass the seals either by removal of the screws or picking of locks. *Id.* at 188.

Mr. Cobb admitted that he did not perform an Open Vulnerability Test, a Penetration Analysis or a Tempest Test because that was outside of the scope of what the Secretary hired him to do. *Id.* at 141-42.[32] Additionally, he did not check whether passwords were hard-coded.

---

[32] A Tempest Test checks for security and secrecy through sound. *See id.* at 143. An Open Vulnerability Test is an open-ended form of testing designed to look for vulnerabilities after

(Continued)

Id. at 154 (explaining that a hard-coded password is when the password is in clear text in the source code). He did not consider the possibility of back-door or trap door passwords on the iVotronic. *Id.* at 155-56; *see id.* at 153 (defining a backdoor password as are "associated with maintenance-type activities where a backdoor password is put in that the maintenance people can get in to do work at a later date). He did not examine whether there were buffer overflow problems remaining in the iVotronic system even though he was aware of a vulnerability that allows the introduction of malicious code through a buffer overflow. *Id.* at 157-159.

During the reexamination of the iVotronic, Mr. Cobb discovered the lock placed over the serial port and compact flash did not prevent access to the compact flash. *See id.* at 186. He recommended that a different type of lock be used. *Id.* at 186-87. He admitted that if his recommendation was not followed, there is a possibility of access to the flash card, *id.* at 189, and that, once accessed, replacement of a compact flash card allows for virus uploading or swapping of votes with fake results. *Id.* at 187-88. Despite the significant potential resulting security vulnerabilities, he did not condition his recommendation on using a different type of lock. *Id.* at 187.

4. There Is A Genuine Issue of Material Fact Concerning Whether Respondent Has Violated The Pennsylvania Constitution (Counts VII, IX & X)

Petitioners have advanced three claims under the Pennsylvania Constitution, specifically under Article I, § 5 (Count VIII),[33] Article I, § 26 (Count IX),[34] and Article VII, § 6 (Count X).[35]

(Continued)

potential attacks have been identified, and Penetration Testing attempts to exploit vulnerabilities that are discovered during the vulnerability test.

[33] Pa. Const. Art. I, § 5 ("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.").

The gist of those claims is that, by certifying EVSs that do not ensure that votes will be honestly captured and counted as cast, Respondent interfered with Petitioners' fundamental right to vote and discriminated against Petitioners and others who are forced to use these DRE machines. Respondent's arguments to the contrary misstate the legal standard, the relevant facts, or both.

a. Respondent Misstates The Nature of Petitioners' Claims and Overstates The Effect of The Prior Summary Judgment Ruling

Respondent characterizes Petitioners' constitutional claims as based ***only*** on their legal claims relating to the "permanent physical record" and "statistical recount" requirements, implying that this Court's prior ruling forecloses consideration of whether DREs violate the law in other ways. *See, e.g.*, Resp't's Supp. Br. at 53 ("Petitioners' ... cause of action was grounded on the legal claim that the Election Code required the Specified Voting Systems to produce voter-verified, software-independent records...."); *id.* at 57-58 ("The import of the Court's opinion is that the Election Code cannot be interpreted to require the types of records and procedures that Petitioners' demand. That holding, combined with the fact that Petitioners have offered no relevant, admissible evidence of lost votes or disenfranchisement, requires judgment in favor of the Secretary."). That is wrong. The fact that the Election Code does not use the term "software independent records" in the definition of "electronic voting system" does not mean that such records are not necessary to preclude tampering as required by the Election Code or to ensure that votes are captured and counted as cast as required by the Constitution. The one does not necessarily follow from the other.

(Continued)

[34] *Id.*, Art. I, § 26 ("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.").

[35] *Id.*, Art. VII, § 6 ("[A]ll laws regulating the holding of elections by the citizens . . . shall be uniform throughout the state.").

Similarly, respondent counters Petitioners' Art. VII, § 1 claims by building a straw man. Specifically, she suggests that Petitioners believe the Constitution "is violated merely because different counties use different voting systems," which is a "mundane and ... meritless claim" because "the fact that different counties use different systems is expressly allowed by the Constitution." Resp't's Supp. Br. at 59-60. Petitioners never made such a claim, however. To be clear, Petitioners' point is not just that these voting systems are "different," but rather that they are different in that some comply with the Election Code and some do not. *See, e.g.*, Petition ¶ 139 (Ex. 1 to Resp't's Supp. Br.) ("[W]hile [Petitioners] are compelled to vote ... using the certified DRE voting systems, other registered voters in Pennsylvania may vote ... using voting systems ... ***that do not suffer from the defects identified in this Petition.***") (emphasis added). Indeed, Petitioners noted this in their own Motion for Partial Summary Judgment, which Respondent has simply ignored: "To be sure, the mere fact that different voters use different voting systems does not in and of itself rise to the level of a constitutional violation, and Petitioners have never argued otherwise." Pet'r's Br. in Supp. of Mot. for Part. Summ. J. dated Sept. 15, 2011, at 58. So did this Court, which Respondent has also simply ignored:

> The Secretary argues that Electors fail to allege an equal protection violation because Article VII, Section 6 of the Pennsylvania Constitution permits the use of voting machines in some parts of the state without requiring the use of voting machines in other parts of the state. ***However, Article VII, Section 6 does not permit DREs that are not reliable or secure and that provide no means for vote verification or vote audit.***

Banfield I, 922 A.2d at 48 (emphasis added) (internal citation omitted).

b. Respondent Misstates The Applicable Legal Standard

Turning to the claims Petitioners actually did raise, Respondent argues that her conduct should be reviewed for whether she has committed a "gross abuse" of power. On the contrary, her conduct implicates a fundamental right and should therefore be subjected to strict scrutiny.

We begin with what should be an unremarkable premise: the right to vote is fundamental. Indeed, having recently taken that very position, Respondent can hardly argue otherwise now. *See, e.g.*, *Applewhite v. Commw.*, 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.").[36]

Nor could any reasonable person, for that matter. Unlike the United States Constitution, our Constitution explicitly recognizes the right to vote. Indeed, it does so in two different places. *See* 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.*, 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 recognized as far back as 1868 that the right to vote is "sacred." *Page v. Allen*, 58 Pa. 338, 347 (1868). Almost a hundred years later, it described that right as "the most treasured prerogative of citizenship." *Appeal of Norwood*, 382 Pa. 547, 549, 116 A.2d 552, 553 (1955). And in the last few decades, this Court and the Supreme Courts of the United States and Pennsylvania have all begun to refer to that

---

[36] Respondent cites Judge Simpson's decision in the *Applewhite* proceeding and claims his decision was "reversed on other grounds." Resp't's Brief at 49. On the contrary, that decision was vacated, not reversed. *See Applewhite v. Commw.*, 54 A.3d 1, at *5 (Pa. Sept. 18, 2012). As such, it should not be cited for any purpose. *See, e.g.*, *Allstate Life Ins. Co. v. Commw.*, 992 A.2d 910, 916 (Pa. Commw. Ct. 2010) ("The Supreme Court vacated, in large part, this Court's opinion and, thus, we have no binding precedent . . . ."). That said, Judge Simpson's decision stood for the proposition that courts can give deference to "the legislature." *See Applewhite v. Commw.*, No. 330 MD 2012, 2012 WL 3332376, at *26 (Pa. Commw. Ct. Aug. 15, 2012). When the challenged state action is not the act of the General Asembly, the Pennsylvania Superme Court has held that no presumption of constitutionality exists. Holt v. 2011 Legislative Reapportionment Comm'm, 39 A.3d 711, 734-35 (Pa. 2012). Ironically, in this case it is the ***Petitioners*** that are asking that the Election Code be enforced as it was written and understood by the legislature.

right as "fundamental." *See, e.g.*, *Bush v. Gore*, 531 U.S. 98, 104 (2000) ("[O]ne source of its fundamental nature lies in the equal weight accorded to each vote and the equal dignity owed to each voter."); *Kuznik*, 588 Pa. at 116, 902 A.2d at 488; *In re Howells*, 20 A.3d 617, 623 (Pa. Commw. Ct. 2011) (noting that absentee voting allowed voters "to exercise their fundamental right to vote"); *In re Zulick*, 832 A.2d 572, 578 (Pa. Commw. Ct. 2003), *aff'd*, 575 Pa. 140, 834 A.2d 1126 (2003) ("Voting is of the most fundamental significance under our constitutional structure") (citing *Burdick v. Takushi*, 504 U.S. 428, 433 (1992)). It follows that this action implicates Petitioners' fundamental right to vote.

Having determined the nature of the rights involved, the question then becomes what degree of scrutiny is given to state action that affects those rights. Respondent suggests that state action affecting the right to vote should be disturbed only if there is a "gross abuse" of power. She is mistaken. Indeed, not one of the cases she has cited for that proposition involved an eligible voter's right to vote. The most glaring example of that is *Finucane v. Pa. Milk Mktg. Bd.*, 136 Pa. Cmwlth. 272, 582 A.2d 1152 (1990), which concerned the General Assembly's decision to set a minimum retail price for the sale of milk. *Id.* at 277-78, 582 A.2d at 1154. Perhaps not surprisingly, that statute was not disturbed. Similarly, while the *Erfer*, *In Re Nomination Papers* and *In Re Zulick* cases concerned ***elections***, they did not concern the right ***to vote*** in an election. *See Erfer v. Commw.*, 568 Pa. 128, 137-38, 794 A.2d 325, 331-32 (2002) (refusing to disturb legislative committee's redrawing of electoral districts in accordance with census data); *In re Nomination Papers of Rogers*, 908 A.2d 948, 955 (Pa. Commw. Ct. 2006) (refusing to disturb requirement that third-party candidates obtain signatures of two percent of voting population of last election in order to be placed on ballot); *In re Zulick*, 832 A.2d at 578 (refusing to disturb statute preventing candidate from running as third-party candidates after

having lost in major-party primary). Indeed, as this Court explained in *In re Zulick,* while "***voting*** is of the most fundamental significance," courts generally have not "recognize[ed] ***candidacy*** as a 'fundamental right.'" *Id.* at 578-79 (emphasis added) (quotation omitted).

When a fundamental right is challenged, Pennsylvania courts will apply strict scrutiny. *See, e.g., James v. Se. Pa. Transp. Auth.*, 505 Pa. 137, 145, 477 A.2d 1302, 1306 (1984) ("[W]here a . . . fundamental right has been burdened, another standard of review is applied: that of strict scrutiny."). This Court has not previously considered the constitutionality of state action when the fundamental right at issue was a qualified elector's right to vote.[37] It stands to reason, though, that the Court would apply the same scrutiny to regulation of "the most treasured prerogative of citizenship" that it would to regulation of other fundamental rights. *Cf. Perles v. Cnty. Return Bd. Of Northumberland*, 415 Pa. 154, 158-59, 202 A.2d 538, 540 (1964) ("The disenfranchisement of even one person validly exercising his right to vote is an extremely serious matter.... [V]oters are not to be dis[en]franchised at an election except for compelling reasons.").

Strict scrutiny requires Respondent to demonstrate that the continued use of these DREs in Pennsylvania is "narrowly tailored to serve a compelling state interest," *DePaul v. Commonwealth*, 600 Pa. 573, 595, 969 A.2d 536, 550 (2009). Respondent's brief does not articulate ***any*** interest, let alone a compelling interest, that is served by keeping these DREs in service in the face of the mounting evidence that they have serious security vulnerabilities that

---

[37] *Mixon v. Commw.*, 759 A.2d 442 (Pa. Commw. Ct. 2000), *aff'd*, 566 Pa. 616, 783 A.2d 763 (2001) comes close. In *Mixon*, this Court considered the constitutionality of preventing currently and recently incarcerated felons from voting in elections. The Court held that the fundamental right to vote was not implicated because currently incarcerated felons were not qualified voters and because the Commonwealth can disenfranchise all felons if it so chose. *Id.* at 451. The Court therefore applied a rational basis standard. Notably, though, the Court nonetheless overturned the enactment denying released felons the right to register to vote, reasoning that there was no rational basis to allow previously registered, released felons to vote and not to allow released felons to register. *Id.* at 452.

permit a motivated attacker to thwart the intent of the voter. Nor has Respondent urged that DREs are necessary to protect the integrity of the democratic process. Her silence on this issue is especially significant because other states have jettisoned these same DREs for systems that create software-independent records.[38]

The use of paperless DREs (whose compliance with the law is specifically disputed) is not the least restrictive means of furthering any purported governmental interest. *See Ins. Adjustment Bureau v. Ins. Comm'r*, 518 Pa. 210, 542 A.2d 1317, 1324 (1988) (restraint on protected speech must be accomplished in least intrusive manner). Indeed, optical scan systems also certified by the Secretary provide greater protection for voters' fundamental right to have their vote captured and counted as cast because of the availability of the record of voter intent that can be used to verify the election results. *See* 2011 Lopresti Report (Ex. 18) at 6.

c. Respondent Misunderstands Which Facts Are "Material"

Having determined the applicable legal standard, the question then becomes whether there are genuine issues of material fact concerning whether Petitioners can satisfy that standard. There are. Respondent's arguments to the contrary rely on a fundamental misunderstanding about which facts are "material."

For example, Respondent suggests that the material fact here is whether Petitioners were "disenfranchised," i.e., that Petitioners cannot state a claim unless they can come to court with some evidence that one of their votes was not honestly captured and counted as cast. *See, e.g.*, Resp't's Supp. Br. at 53. While such evidence would certainly be ***one*** way to state a claim,

---

[38] *See e.g.* FLA. STAT, ch. 101 §56075 (2012) (requiring all voting to be by Marksense optical scan technology and superseding *Wexler v. Lepore,* 87 So.2d 1276 (Fla Dist. Ct. App. 4th Dist. 2004)); CAL. ELEC. CODE § 19250 (2012) (superseding *Weber v. Shelley,* 347 F.3d 1101 (9th Cir. 2003)); MD. CODE. ANN. ELEC. §9-102 (2012) (superseding *Schade v. Maryland State Bd. of Elections,* 401 Md. 1 (2007)). It should also be noted that the decisions Respondent cites in her brief were decided before the vulnerabilities of DREs were widely known. *See supra.*

it is certainly not the ***only*** way to state a claim. As it happens, this Court already found as much. Specifically, Respondent made this same argument at the preliminary objection stage, suggesting that Petitioners had not stated a claim for relief because they did not plead disenfranchisement. The Court rejected the premise of that argument:

> [T]he Secretary argues that this court should dismiss Count VIII of the Petition for failure to plead a constitutional injury.... Because Electors have a right under Article I, Section 5 of the Pennsylvania Constitution to have their votes honestly counted and because Electors have no way of knowing whether their votes will be honestly counted by DREs that are not reliable or secure and that provide no means for vote verification or vote audit, Electors have pled an injury under Article I, Section 5....
>
> [T]he Secretary argues that this court should dismiss Count IX of the Petition for failure to allege the denial of a right.... Because Electors have a right to vote and because Electors have no way of knowing whether using the DREs affords them that right, Electors have pled the denial of a civil right under Article I, Section 26.

Banfield I, 922 A.2d at 48-49. If Petitioners could survive dismissal by pleading that they had no way of knowing whether their votes would be captured and counted as cast, it follows that they can survive summary judgment by offering evidence to that effect. Respondent can deride the "no way of knowing" theory of liability as an "empty mantra" all she wants, Resp't's Supp. Br. at 51, but that will not change the fact that an *en banc* panel of this Court has clearly endorsed it. If she disagrees, she may pursue the issue on appeal. For the time being it is the law of the case – much as the Court's recent decision that DREs satisfy the "permanent physical record" and "statistical recount" provisions is the law of the case no matter how much Petitioners may disagree with it.

In light of this Court's prior rulings and the precedent on which it relied, the disputed material fact (or at least one of them) is whether Petitioners have any "way of knowing whether their votes will be honestly counted by DREs that are not reliable or secure. . . ." *Banfield I*, 922

A.2d at 48. And as to ***that*** material fact, there are at a minimum genuine issues that preclude the entry of summary judgment. *See infra* Section IV.B.4.d.

d. Respondent Ignores Genuine Disputes Concerning The Material Facts

The record makes clear that Petitioners have adduced substantial evidence demonstrating a genuine dispute concerning the material facts. Petitioners have established, through expert testimony and published scientific papers that the DREs at issue do not preclude tampering with the tabulating element as required by the Election Code or tampering with ballots. *Supra* § B. And, there is a genuine dispute of material fact whether the Secretary's re-examinations testing complied with every requirement of the Election Code, particularly the Security requirements. *See supra* § 3.

Respondent makes no mention of that evidence. Instead, she simply demeans Petitioners' concerns as "flights of imagination," "imagined fears," and so on. Resp't's Supp. Br. at 51, 52. Indeed, she even goes so far as to say that DREs "have not failed to register or count votes during any election; they have not been tampered with or manipulated during any election they have not malfunctioned in such a way as to deny voters their right to vote." *Id.* at 58; *see also id.* at 3 ("The machines accurately and correctly registered, recorded, and tabulated each vote…."). That is intellectually dishonest. The most she can say (as she does throughout her brief) is that there is no ***evidence*** of votes being lost or manipulated. Why? Because as she herself argued, the only "recount" DREs can perform cannot determine whether a vote was accurately captured. *See* Resp't's Opp'n to Mot. for Partial Summ. J. dated Oct. 14, 2011, at 47 ("It is not designed to be a forensic examination into whether a voter's intent was properly recorded by the machine."). The secret ballot is a time-honored part of our electoral system, the consequence – indeed, the purpose – of which is that only one person on Earth – the voter – knows how a vote was cast. When that person leaves the polling place, it is impossible to match up voter and vote. It follows

that the only way to be able to verify that a voter's intent was captured correctly is to create a permanent physical record of it the moment it is cast. DREs simply cannot do that. Instead, the best they can do is print something out days or weeks later, after the data have been mediated by the firmware, software, and by extension anyone who had access to either of them.

At the risk of stating the obvious, Petitioners disagree with the Court's conclusion that such systems satisfy the "permanent physical record"[39] and "statistical recount"[40] requirements. Indeed, it is commonly understood that paperless election results such as those produced by lever machines and DREs can at most be "recanvassed,"[41] which is fundamentally different from being

---

[39] Before this litigation arose, even Respondent's own expert seemed to accept the commonsense notion that paper ballots are "physical" and electronic data is, well, "electronic." *See, e.g.*, Hearing Before the Texas House Committee on Elections (Nov. 25, 1986) (Ex. 16) at P-15773-74 (discussing punch card machines) ("When you're ready 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 – on a roll of paper tape so that it can be reconstructed later. It's also recorded electronically in two different ways…").

[40] *See* Petitioners' Summary Judgment Briefs dated September 15 and November 1, 2011; *see also* Candice Hoke, *Chapter 17: Voting Technology and the Quest for Trustworthy Elections*, *in America Votes! A Guide to Modern Election Law & Voting*, Section I: Background: Performance Records of E-Voting Systems (Benjamin E. Griffith, 2nd ed. 2012), available on Westlaw at ABA-AMVOTE § 17.1 ("All-electronic DRE touchscreen unites that produce no contemporaneous voter-verified paper record have received the most pointed criticism. The most widely endorsed e-voting systems require voters to mark a paper ballot that is then read by an optical scanner with vote tallies . . . [which] permit the extrinsic paper record to be used to verify or correct the software-produced vote tallies in post-election audits or recounts."); *id.* at Section V: Moving Forward ("Post-election auditing or 'recounting' using paper ballot records can provide the independent check on the voting machines. 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.").

[41] *See, e.g.*, *In re Gen. Election for Twp. Supervisor*, 152 Pa. Commw. 590, 596, 620 A.2d 565, 568-69 (Pa. Commw. Ct. 1993) ("A recount is the opening of a ballot box and the recount of the votes if the voting was done by paper ballots. A recanvass is the opening of a voting machine in order to check the counters inside the machine which record the number of votes cast if the voting was done by voting machines."); 22 Pennsylvania Law Encyclopedia § 105 (Matthew Bender & Co., 2nd ed. 2011) ("There are several methods by which the asserted results of an election may be challenged. Ballots may be recounted and voting machines may be recanvassed on allegations of fraud or mistake.").

"recounted."[42] But even accepting the Court's conclusion for present purposes, it does not necessarily follow that DREs allow anyone to know that their votes have been captured and counted as cast. Indeed, Respondent is confident that DREs will do that: "if the voting system performs according to its design ... which it can be expected to do after it passes pre-election testing." Resp't's Opp'n to Mot. for Partial Summ. J. at 18. Of course, the flip-side of that is also true. That is, if a DRE does not perform according to its design, if it is compromised after pre-election testing (which by definition happens before an election), then one can never know, even if a purported "recount" is performed, that a vote was captured and counted as cast.

Given the availability of other EVSs that do not pose the same problems as DREs, Respondent's conduct is not likely to satisfy strict scrutiny. If for example her office is trying to save the counties the expense of replacing or retrofitting DREs – an understandable motivation,[43] to be sure – that would not pass muster under the Constitution. *See Saenz v. Roe*, 526 U.S. 489, 507 (1999) ("[T]the State's legitimate interest in saving money provides no justification for its decision to discriminate among equally eligible citizens...."). For present purposes, though, the only thing that matters is whether there are genuine issues of material fact. And the answer to that question is "yes."

---

[42] *See* 25 Pa. Stat. Ann. § 3031.17 ("The county board of elections . . . 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."). As Dr. Shamos said, if a "voter's intentions were frustrated" before her vote was captured, "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...." Hearing Before the Texas House Committee on Elections (Nov. 25, 1986) (Ex. 16) at P-15740-42.

[43] To Petitioners' knowledge, Respondent has not analyzed the costs of replacing DREs. As for retrofitting them with a mechanism for creating a non-sequential voter-verified paper audit trail that would not compromise the secret ballot, Respondent has estimated that "it would cost approximately 25 million dollars for all Pennsylvania counties to upgrade their DRE systems." Boehm Mem. (Ex. 31) at 7.

V. CONCLUSION

For the foregoing reasons, Petitioners respectfully request that Respondent's Application for Summary Relief be denied.

Respectfully submitted,

DATED: April 11, 2013

Michael P. Daly (Id. No. 86103)
Meredith N. Reinhardt (Id. No. 93504)
Katie L. Bailey (Id. No. 308748)
DRINKER BIDDLE & REATH LLP
One Logan Square, Suite 2000
Philadelphia, PA 19103-6996
Phone: 215.988.2700
Fax: 215.988.2757

Marian K. Schneider (Id. No. 50337)
Attorney-at-Law
295 E. Swedesford Road, #348
Wayne, PA 19087
Phone: 610.644.1255
Fax: 610.644.1277

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
Phone: 215.627.7100
Fax: 215.627.3183

Counsel for Petitioners Mark Banfield et al.

CERTIFICATE OF SERVICE

I certify that, on April 11, 2013, I caused a true and correct copy of the foregoing document to be served on the following via First Class and electronic mail:

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 Respondent

Daniel J. Fischer
Michael Cox
Koley Jessen P.C., L.L.O.
1 Pacific Place, Suite 800
1125 S. 103rd St.
Omaha, NE 68124

Joseph Uhl Metz
Victor Stabile
Dilworth Paxson LP
112 Market St., Suite 800
Harrisburg, PA 17101

Attorneys for Election Systems & Software

Peter D. Kennedy
401 Congress Ave., Suite 2200
Austin, TX 78701

Chris Fisher
Tucker Arensberg
2 Lemoyne Drive, Suite 200
Lemoyne, PA 17043

Attorneys for Hart InterCivic, Inc.

Dated: April 11, 2013

Katie L. Bailey