NOT FOR PUBLICATION WITHOUT THE APPROVAL OF THE
COMMITTEE ON OPINIONS

ASSEMBLYMAN REED GUSCIORA, STEPHANIE HARRIS, COALITION FOR PEACE ACTION, and NEW JERSEY PEACE ACTION, Plaintiffs, v. JON S. CORZINE, GOVERNOR OF THE STATE OF NEW JERSEY, (in his official capacity) and NINA MITCHELL WELLS, SECRETARY OF STATE OF THE STATE OF NEW JERSEY (in her official capacity), Defendants.	SUPERIOR COURT OF NEW JERSEY LAW DIVISION-MERCER COUNTY DOCKET No.:MER-L-2691-04 CIVIL ACTION OPINION

Decided: February 1, 2010

Penny M. Venetis, for the plaintiffs (Rutgers Constitutional Litigation Clinic, attorneys; Ms. Venetis, on the brief).

John McGahren and Caroline F. Bartlett, for the plaintiffs (Patton Boggs, attorneys; Mr. McGahren and Ms. Bartlett, on the brief).

Paula T. Dow, Acting Attorney General, for the defendants (Leslie M. Gore, Assistant Attorney General; Donna J. Kelly, Assistant Attorney General; Jason S. Postelnik, Deputy Attorney General; Brian G. Flanagan, Deputy Attorney General; and Victor N. DiFrancesco, Jr., Deputy Attorney General, attorneys; Ms. Gore, Ms. Kelly and Mr. Postelnik, on the brief).

Arthur Chagaris, George A. Campion and Annalisa Siracusa for Sequoia Voting Systems (participated in a limited capacity); (Beattie Padovano, attorneys).

FEINBERG, A.J.S.C.

I.

BACKGROUND

On October 19, 2004, Mercer County Assemblyman Reed Gusciora; Stephanie Harris, a registered voter in Mercer County; and two citizens' organizations – the Coalition for Peace Action and New Jersey Peace Action (collectively "plaintiffs"), filed a complaint in lieu of prerogative writs and order to show cause seeking to restrain the use of direct recording electronic ("DRE") voting machines in this State. The complaint named former Governor James E. McGreevey and former Attorney General Peter C. Harvey as the State's Chief Election Official, in their official capacities ("defendants" or "State").[1]

Since the inception of this litigation over five years ago, this court has addressed a myriad of procedural and substantive issues set forth in numerous written and oral opinions. These have arisen in the context of: (1) multiple orders to show cause seeking temporary restraints; (2) a remand from the Appellate Division directing the court to conduct a hearing regarding the feasibility of the State meeting the statutory deadline to implement a DRE with a voter verified paper audit trail ("VVPAT")[2]; (3) the request, as part of the remand hearing, for the court to determine the criteria to be applied if the State sought a waiver; (4) a decision by the Appellate Division directing the Law Division to monitor compliance with the statutory mandate that the State satisfy the requirement that each voting machine produce a VVPAT; and (5) a trial that commenced on January 27, 2009 and ended on May 11, 2009, that focused on the AVC Advantage ("AVC") made by Sequoia Voting Systems ("Sequoia").[3]

---

[1] Counsel for the parties, in their trial summations, list the parties as former Governor Jon C. Corzine and former Secretary of State Nina Mitchell Wells. There is, however, no order in the court's file or on the Automated Civil Case Management system to establish that the complaint was formally amended.

[2] The remand hearing addressed ten voting machines manufactured by three different companies: (1) Sequoia Edge; (2) Sequoia Edge/VVPAT; (3) Sequoia AVC Advantage; (4) Sequoia AVC Advantage/VVPAT; (5) ES&S iVotronic; (6) ES&S iVotronic-RTAL; (7) ES&S RTAL with a cut-and-drop system; (8) ES&S Precinct Based Optical Scanner; (9) AVANTE Vote-Trakker EVC 308-SPR; and (10) AVANTE Vote-Trakker EVC 308-FF.

[3] The Sequoia Edge, made by Sequoia, is used in one county. With the Sequoia Edge the voter is required to go through multiple pages to view all of the different contests and candidates. The AVC, a full-face

During four and one-half years of the pre-trial phase of the litigation, the court had the opportunity to review certifications from election officials throughout the State. At trial, the witnesses included private citizens, State and County election officials, members of the Title 19 Committee, N.J.S.A. 19:48-2, and well-known computer science experts. Without exception, each of the trial witnesses has contributed to the court's understanding and appreciation of how voters in this State cast their votes. The attorneys in this case were well-prepared and dedicated significant time and energy to present their respective positions. I am grateful to have had the opportunity to have these fine men and woman appear before me.

II.

PRE-TRIAL PROCEDURAL HISTORY

As noted heretofore, when the complaint was filed plaintiffs sought to: (1) enjoin the use of DREs in the November 2004 general election; (2) require that all DREs be retrofitted to provide a VVPAT after the November election; (3) require all new DREs purchased in the State to be equipped with a VVPAT; and (4) grant reasonable attorney's fees and costs. R. 4:52-1 et seq.

The complaint, consisting of eighty-nine paragraphs, alleged the continued use of DREs violated: (1) the Constitutional requirement in N.J. Const. Art. II, ¶ 3(a) that every vote be counted; (2) the guarantee of Equal Protection in N.J. Const. Art. I, ¶ 1; (3) the statutory guidelines for recounts found in N.J.S.A. 19:28-1 et seq.; (4) the statutory requirement that each voter's intent be tabulated in accordance with N.J.S.A. 19:48-1(d) and (f) and N.J.S.A. 19:53A-3(b); (5) the statutory requirement that voting equipment be secure as mandated by N.J.S.A. 19:53A-3(g); and (6) the statutory requirement that votes be counted accurately under N.J.S.A. 19:48-1(h) and N.J.S.A. 19:53A-3(h).

On October 25, 2004, the State filed a cross-motion to dismiss. R. 4:6-2(e). In support of its application, the State filed approximately three hundred pages of certifications from forty-two election officials from counties around the State. This included County Clerks, Superintendents of Elections and

---

machine, permits the voter to view the entire ballot on one surface. The full-face, in that respect, is similar to the former lever machine.

Boards of Elections. The State also filed certifications from each of the three manufacturers of voting systems.

In its motion to dismiss, the State raised procedural and substantive grounds: (1) the court lacked jurisdiction; (2) the action was time barred; (3) plaintiffs failed to include indispensable parties: to wit, County Clerks, County Boards of Elections and County Superintendents of Elections; (4) plaintiffs lacked standing; (5) the doctrine of laches precluded emergent relief; (6) judicial policy disfavored belatedly filed requests for injunctive relief which could disrupt a forthcoming election; (7) certified voting machines are presumed valid, N.J.SA. 19:48-2; and (8) plaintiffs failed to establish any basis for injunctive relief. R. 4:52-1 et seq.

The filing of this action, thirteen days prior to the election, necessitated an expedited briefing schedule and hearing date. On October 26, 2004, in a fifty-five page opinion, the court denied injunctive relief and denied, without prejudice, the cross-motion to dismiss the complaint. R. 4:52-1; R. 4:6-2(e). The court held:

> In sum, the balance of equities clearly favors denial of the relief requested. As the certifications submitted by the State demonstrate, switching to a system of paper ballots at this late date in 21 counties is logistically impossible. The speculative concerns regarding electronic voting machines pales in comparison with the very real threat of voter confusion and an inability to conduct an orderly and secure election process on November 2, 2004.
>
> [Gusciora v. McGreevey, No.: MER-L-2691-04, (10/6/2004), pp. 54-55.]

On November 15, 2004, plaintiffs filed a motion to modify the denial of injunctive relief, R. 4:52-1 or, in the alternative, to amend the findings by the court. R. 1:7-4(b). On December 2, 2004, the State filed opposition and again moved to dismiss the complaint in lieu of filing an answer. R. 4:6-2(e). In an opinion issued January 13, 2005, the court granted defendants' motion to dismiss with prejudice.

The court entered judgment on January 27, 2005, and an appeal followed. While the appeal was pending in July 2005, the Legislature enacted and the Governor signed, P.L. 2005, c. 137. This statute required that all voting machines produce a VVPAT by January 1, 2008.

The 2005 amendment codified both in N.J.S.A. 19:48-1 and N.J.S.A. 19:53A-3, provided, in relevant part:

> [b]y January 1, 2008, each voting machine shall produce an individual permanent paper record for each vote cast, which shall be made available for inspection and verification by the voter at the time the vote is cast, and preserved for later use in any manual audit. In the event of a recount of the results of an election, the voter-verified paper record shall be the official tally in that election. A waiver of the provisions of this paragraph shall be granted by the Attorney General if the technology to produce a permanent voter-verified paper record for each vote cast is not commercially available.
>
> [N.J.S.A. 19:48-1; N.J.S.A. 19:53A-3 (emphasis added).]

In addition, P.L. 2005, c. 137 (A-33) added the following new section as N.J.S.A. 19:53A-3.1:

> [u]nless federal funding is made available to pay for the purchase or retrofit of a voting machine to produce a voter-verified paper record as required by P.L. 2005, c. 137 (C.19:48-1 et al.), a county shall be reimbursed by the State for such costs upon application for reimbursement to the Attorney General and approval of the application by the Director of the Division of Budget and Accounting in the Department of the Treasury, in accordance with the provisions of Article VIII, Section II, paragraph 5 of the New Jersey Constitution.
>
> [N.J.S.A. 19:53A-3.1 (emphasis added).]

As a result of the newly adopted statutes, the Appellate Division directed the parties to submit additional briefs on the question of whether the appeal was moot. On January 25, 2006, the issue was argued before the Appellate Division. In light of the legislation requiring all voting machines to produce a VVPAT on or before January 1, 2008, the Attorney General argued the appeal was moot. In response, plaintiffs argued the uncertainty of the implementation date, coupled with the fact that elections would occur before the implementation date, left the constitutional issues unresolved.

On February 9, 2006, the Appellate Division remanded the matter to the Law Division. To assist in determining whether the issue was moot, the Appellate Division directed the court to consider whether the technology and resources were available to implement P.L. 2005, c. 137. Inasmuch as the legislation

provided for the type of ballot verification sought in the complaint, the Appellate Division sought an expedited determination by the Law Division.

The Appellate Division also directed the new Administration and the Attorney General to address the criteria for development of guidelines to grant waivers under the statute. Finally, the Appellate Division ordered the Law Division to file its findings on or before April 21, 2006.[4] Consistent with the above, on February 15, 2006, the court held an initial case management conference and established dates for the exchange of witness lists and experts reports, if any, the filing of pre-trial briefs, and the date(s) for the remand hearing. Four subsequent case management conferences were held in March 2006. The remand hearing commenced on March 16, 2006 and continued on March 17, 20 and 23, 2006. Six witnesses testified and twenty-nine exhibits were admitted into evidence. The court directed the parties to file recommended findings of fact on or before March 24, 2006.

The forty-nine page remand opinion, issued on April 19, 2006, included a comprehensive review of each of the voting machines used in the State. At the time of the remand, AVANTE was the only company that offered a voting system that produced a VVPAT.[5] A representative from AVANTE testified that the company was awaiting federal certification for a full-face, cut-and-drop machine that produced a VVPAT.[6] Given the uncertainty of the commercial availability of the AVC with a VVPAT by January 1, 2008, the court concluded that the Office of Legislative Services may have grossly underestimated the cost to purchase or retrofit voting machines utilized in the State. While the State argued the court was without the authority to compel the Legislature to expend these funds, the new Administration and the Attorney General represented their firm committment to implement the statutory mandate to provide a VVPAT by January 1, 2008.

---

[4] From February 2006 to the commencement of trial, January 27, 2009, the court addressed the availability of a DRE with VVPAT from three different manufactures. During the trial, the court focused specifically on the AVC. The AVC, manufactured by Sequoia, is used in eighteen of the twenty-one counties. Unless otherwise noted, reference to the AVC is the AVC Version 9.00H.

[5] AVANTE offered a reel-to-reel system. A reel-to-reel system provides a paper ballot on a cylindrical reel that records votes sequentially. The reel-to-reel system has raised concerns regarding voter secrecy.

[6] In a cut-and-drop system the paper ballot is cut and dropped into a receptacle.

Based on the record established during the remand, the court concluded that the availability of a VVPAT by January 1, 2008 was questionable. Furthermore, the court predicted that the cost to purchase new machines would exceed the estimated $21 million.

On May 24, 2006, the matter was re-argued before the Appellate Division. On June 29, 2006 the Appellate Division held that "every perceived constitutional deficiency in the electoral process would be remedied by a timely and successful implementation of the new law." Gusciora v. McGreevey, 395 N.J. Super. 426 (App.Div. 2006). The court vacated the dismissal of the complaint and remanded the matter to the Law Division to conduct such case management conferences and hearings as necessary to monitor compliance with the new legislation. The Appellate Division held that only plaintiffs' constitutional "issue would remain if the VVPAT legislation is not timely and successfully implemented." Ibid.

Consistent with the June 29, 2006 decision by the Appellate Division, on August 24, 2006 the court held a case management conference to establish a monthly compliance review schedule. On September 5, 2006, the court entered an order requiring the State to provide monthly written status reports on the progress of VVPAT development and implementation. According to case management records, between September 5, 2006 and the first day of trial, January 27, 2009, the court held approximately thirty case management conferences.

In the summer and early fall of 2007, as the January 1, 2008 deadline approached, the court directed the State to retrofit existing machines with a VVPAT or find suitable alternatives. During the same period, plaintiffs moved to bar the use of DREs without a VVPAT in the next election. During a case management conference on September 17, 2007, the State advised the court that it was unlikely the VVPAT would be ready by the statutory deadline. The State placed on the record the steps it had taken to meet the statutory deadline. Part of that effort included the unprecedented step, undertaken by the State, to enter into an agreement with the New Jersey Institute of Technology to test and evaluate voting machines with a VVPAT. N.J.S.A. 19:48-1; N.J.S.A. 19:53A-3.[7]

[7] Early in 2006, on the record, this court recommended to the State that a private or public academic institution, professional organization or entity be considered to review and provide recommendations.

At the compliance hearing, the Attorney General explained three options. These included: (1) retrofit existing DREs with VVPATs by the statutory deadline; (2) purchase a new voting system (precinct-based optical scanners) and implement the new system in each of the twenty-one counties by the statutory deadline; or (3) utilize a paper ballot system in place of VVPAT until these machines became available.

As part of the deliberations, the Attorney General represented that numerous discussions had taken place with interested stakeholders, including legislative leaders, the County Superintendents of Elections, County Boards of Elections, County Clerks, the Public Advocate, voting machine vendors and members of the advocacy community. This collaborative effort was undertaken to identify issues attendant to each of these options.[8]

After reviewing these options, the Attorney General determined that none were realistic. As a result, for the February 2008 election, the Attorney General recommended continued use of DREs pending final certification of new voting machines equipped with a VVPAT. While the State acknowledged the possibility of meeting the statutory deadline, the State also cautioned that the training

---

[8] At times, the offices of the County Clerk ("Clerk"), Board of Elections ("Board") and Superintendent of Elections ("Superintendent") have been used almost interchangeably. In fact, while their roles often interact with one another, their duties are quite different. To avoid confusion, the role of each of these offices is explained briefly. The Clerk, an elected official, handles election-related matters. In this capacity, the Clerk: (1) receives petitions for offices; (2) designs and prints all election ballots; (3) prepares and prints the sample ballot; (4) draws lots for ballot position; (5) approves or rejects mail-in ballots; (6) prints and issues mail-in ballots; (7) prints and supplies emergency and provisional ballots; (8) tabulates the votes; and (9) certifies the election. The Superintendent, appointed by the Governor, also referred to as the Commissioner of Registration: (1) accepts voter registrations; (2) reviews and approves voter registrations; (3) receives and stores provisional ballots after the election; (4) verifies registration for all provisional ballots; and (5) acts as the custodian for the voting machines. As custodian, the Superintendent is responsible for the maintenance, storage, and delivery of the voting machines. A Superintendent is required in all 1st class counties and permitted in 2nd and 5th class counties. Superintendents are currently in Atlantic, Bergen, Burlington, Camden, Essex, Hudson, Mercer, Monmouth, Morris, and Passaic Counties. The Board is responsible for: (1) selection of polling places; (2) enforcement of the Accessibility Act; (3) creation and maintenance of election districts; (4) appointment of challengers; (5) appointment and training of board workers; (6) receiving, counting, investigating, and certifying mail-in ballots; and (7) counting and certifying provisional ballots. In counties where there is no Superintendent, the Board also handles all of the responsibilities of Superintendent.

of election officials, on the use of a new voting system, was unlikely before the February 2008 presidential primary. In response, plaintiffs sought an order from the court to require the State to purchase, in all twenty-one counties, precinct-based optical scan voting machines.[9]

Prior to the September 17, 2007 compliance review hearing, attorneys for the Republican and Democratic State Committees ("State Committees"), as well as many State and County election officials, expressed unanimous support to extend the statutory deadline. Counsel for the State Committees appeared before the court on September 17, 2007 to support the application of the State. At the hearing counsel for the State Committees, along with County and State election representatives, urged the court to reject the recommendation by plaintiffs to abandon DREs and to purchase precinct-based optical scanners.

The court denied plaintiffs' application to bar the use of DREs and to switch to precinct-based optical scan voting machines. In the October 9, 2007 order, denying relief, the court deferred setting a hearing date to address the constitutional issues pending the next scheduled case management conference. On December 7, 2007, satisfied that the State would not meet the statutory deadline, the court established a discovery order as part of the pre-trial process. A confirmatory order was signed on January 7, 2008.

As anticipated by the court, the State did not meet the VVPAT deadline. On or about January 13, 2008 the VVPAT deadline was extended to June 13, 2008. P.L. 2007, c. 301 (S-2949). One month before the June 13, 2008 deadline, the Legislature changed the date for VVPAT records of votes cast on voting machines to be in place to January 1, 2009. P.L. 2008, c. 18 (A-2229). The bill also amended the current law to shift responsibility for the administration of certain election procedures from the Attorney

[9] While plaintiffs initially requested that each DRE be equipped with a VVPAT, at this stage of the proceedings and throughout the trial, plaintiffs modified the request to require the State to purchase precinct-based optical scanners.

General to the Secretary of State, in conformity with P.L. 2007, c. 254 (C.52:16A-98), which effectuated that change.[10]

Prior to the first day of trial on January 27, 2009, the court addressed more than thirty pre-trial motions. One of these, raised by counsel for Sequoia, objected to the release of proprietary and confidential information to plaintiffs' expert.[11] After several iterations of a protective order and with the assistance of the court, the parties ultimately agreed to the terms and conditions of an order. In part, the protective order permitted plaintiffs' experts to examine the voting machines at the New Jersey State Police ("NJSP") Headquarters during the summer of 2008.

The court rejects the notion by the State that this court took "unprecedented action" in ordering the release of the source code. First, release of the source code was necessary in order to provide plaintiffs' experts with the opportunity to examine the AVC. Second, the months expended by this court to assist the parties in drafting a protective order, fully safeguarded the interests of Sequoia. Third, in State v. Chun, 194 N.J. 54, 70 (2008), in a case similar to the one before this court, the Court issued an order to compel the manufacturer of a computerized breathalyzer test to allow the firmware and source code of the device to be analyzed.

This opinion, due to space constraints, does not include the court's findings on numerous pre-trial and trial motions. The facts and issues identified in these motions and cross-motions are set forth in the papers submitted by the parties, the many writen and oral opinions issues by this court and the arguments placed on the record by the parties during oral argument. Suffice it to say, these are all part of the official court record.

On the first day of trial, the court addressed approximately twenty motions. One of the applications related to the role of Sequoia. While Sequoia was not named as a defendant, counsel for

---

[10] During the trial, which began on January 27, 2009, the State represented that on January 5, 2009 the Secretary of State certified the AVC VVPAT record system with firmware Version D-10 for use in any election within the State. N.J.S.A. 19:53A-4.

[11] Specifically, Sequoia objected to the release of the source code.

Sequoia moved for permission to participate as a party. R. 4:28-1; R. 4:29-1.[12] Given the lateness of the motion, the court denied the application. The court permitted Sequoia to continue, at trial, in its limited role to raise issues covered by the protective order.

When the trial commenced, legislation had already been introduced to suspend the VVPAT implementation date indefinitely. The trial ended on May 11, 2009, spanning a period of twenty-five days. Mid-way into the trial, March 6, 2009, the Governor signed into law P.L. 2009, c. 17, which indefinitely suspended VVPAT implementation, until such time as:

> [t]he Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State to offset the entire cost of ensuring that each voting machine used in this State produces an individual permanent paper record for each vote cast; or (2) the annual appropriation act contains an appropriation of sufficient funds to ensure that each voting machine used in this State produces an individual permanent paper record for each vote cast and such appropriated funds have not been reserved by the Governor under a spending reduction plan; or (3) the Secretary of State and the State Treasurer certify in writing that sufficient funds have been provided by the federal government and received by the State, and the annual appropriation act contains an appropriation of sufficient unreserved funds, to ensure, when such funds are combined, that each voting machine used in this State produces an individual paper record for each vote cast.
>
> [Ibid.]

The reasons set forth in the sponsor's statement outlines the specific fiscal reasons for the delay in the implementation:

> [t]he sponsor's statement attached to the bill indicates that the suspension is necessary because of the economic situation in the State. The State anticipates a $2.1 billion budget gap in fiscal year 2009 and a more severe gap in fiscal year 2010. Although $19 million in State funds had been set aside to help pay the costs of retrofitting the direct recording voting machines used in eighteen of the State's twenty-one counties, this money is no longer available for that purpose. The funds have been placed in reserve to help the State meet its budgets, as required by the New Jersey Constitution. Without this $19 million, there are insufficient funds available currently to pay for a retrofit of all the DRE voting machines or to change to any other alternative voting system that produces a paper ballot.

[12] Prior to trial, Sequoia sought to limit its role to pre-trial discovery issues.

[Ibid.]

On May 11, 2009, the last day of trial, the court established a briefing schedule. Consistent with that schedule, counsel for plaintiffs filed recommended findings of fact and conclusions of law on July 5, 2009. Defendants filed recommended findings of fact and conclusion of law on September 21, 2009. With the consent of the State, the court granted plaintiffs' request to extend the time to file a rebuttal brief to November 20, 2009.

III.

TRIAL

Sixteen witnesses testified and 129 exhibits were admitted into evidence. Each of the ten lay expressed a sincere interest in the integrity and reliability of the voting process. Furthermore, while the six expert witnesses differed, in part, each one was professional and well-prepared. Given the nature of the issues, it is important to this court that voters have a basic understanding of how voting machines operate, and the procedures that take place before, during and after an election. As a result, what follows is a comprehensive review of the testimonial and documentary evidence offered at trial.

While this opinion is 276 pages long, the trial record consists of over four thousand pages of transcripts and approximately two thousand pages of expert reports and post-trial submissions filed by the parties. This does not include motions and transcripts from October 2004 to the first day of trial.

A summary of the testimony of the lay witnesses is presented first. The testimony of the expert witnesses follows, in order of their appearance. At the request and consent of counsel, to accommodate the schedule of witnesses, the court permitted witnesses to testify out of turn.

1. STEPHANIE HARRIS (WITNESS FOR PLAINITFFS)

Plaintiff, Stephanie Harris ("Harris"), is a resident of Mercer County. On June 8, 2004, the day of the Presidential primary, Harris entered the voting booth, pressed the buttons next to the names of the candidates she wished to elect, activated the "cast vote" button, and exited the voting booth. After exiting the voting booth, a poll worker advised Harris the votes did not register and directed her to return to the voting booth to vote again. After exiting the voting booth a second time, the poll worker again directed

Harris to return to the voting booth to vote. The same scenario occurred a third time. After voting a fourth time, the poll worker said, "I think it counted."[13] Tr. 73:17, Jan. 27, 2009.

Since June 8, 2004, but for one occasion, Harris has voted by absentee ballot. On that one occasion, between 2006 and 2007, Harris voted without incident. As a result of her experience on June 8, 2004, Harris has become active in election reform by working to pass voter verification and audit legislation.

2. PROFESSOR EDWARD FELTON (WITNESS FOR PLAINTIFFS)

Professor Edward Felton ("Felton") is a faculty member in the Computer Science Department and Woodrow Wilson School of Public Policy at Princeton University. A resident of Mercer County, Felton has voted on the AVC since November 2004. Felton testified as a fact witness.

In November 2004, November 2006, and February 2008, Felton photographed unattended voting machines in the lobby of an elementary school and a social hall located in the basement of a church. On each occasion, Felton entered the building through an unlocked door and examined machines without interruption. According to Felton, he did not observe security cameras or security personnel on site.

Prior to the June 2008 Presidential primary on June 1, 2008 and June 2, 2008, Felton observed eighteen unattended machines at five public polling places. At each location, the buildings were open. After entry, Felton examined the voting machines and photographed the unattended machines. On June 2, 2008, at four of the polling places, Felton observed prominent signs inside and outside of the buildings. The signs directed members of the public to the whereabouts of the unattended voting machines. Regarding the content of the signs, Felton testified, "I don't recall exactly, but it was something like "Park Here to Vote." Tr. 47:8-9, Feb. 10, 2009.

3. JAMES CLAYTON (WITNESS FOR THE STATE)

James Clayton ("Clayton"), a graduate of Richard Stockton College, is currently enrolled in a Master's degree program in History at Monmouth University. Since 1997, Clayton has worked for the

[13] For convenience, when referring to transcripts, the date of trial will be listed once for witnesses who testified on one day. Transcript references when a witness testified on multiple days are noted as Tr. 1, for the first day, Tr. 2, for the second day and repeated sequentially, as appropriate.

Ocean County Board of Elections. Initially hired as a voting machine mechanic, Clayton's duties included maintaining and preparing the voting machines for upcoming elections and arranging the transportation of the voting machines to and from polling places. Other than on-site training offered by staff and by Sequoia, Clayton has no training in computer engineering or computer security. Clayton is a member of the New Jersey Association of Election Officials (the "Association"), an advocacy group comprised of the State's election officials and administrators. He serves on the Association's voting machine committee.

Since 1999, Clayton has served as the Coordinator of the Voting Technology Center. Clayton, a Republican, and Dolores Zimmerman ("Zimmerman"), a Democrat, supervise a staff of six permanent full-time employees and four part-time seasonal employees. In 1996 Ocean County purchased 600 AVC voting systems. Currently, the County owns 818 AVC voting systems divided among 384 election districts.

Clayton testified that the Clerk's office prepares and designs the ballot face. Once completed by the Clerk, Clayton and Zimmerman, trained by Sequoia in WinEDS, enter the ballot information into WinEDS enabled laptop computers.[14] The laptops and results cartridges are kept in separately locked rooms at the warehouse. Only Clayton and Zimmerman have keys. Each results cartridge is examined before an election to make sure it is ready to receive new information. Once placed into a cartridge reader, whatever data is on the results cartridge is cleared. Each machine has one results cartridge and, if the machine is audio-enabled, the machine is equipped with an audio-cartridge.[15] The computers used to prepare the results cartridges for the voting machines are never connected to the Internet.

---

[14] WinEDS, a windows based program combined with an election data system, designed by Sequoia, runs on computers at election central. It defines the ballot formation and manages voting machines. Through WinEDS, results cartridges with the election definition are established and placed into voting machines to prepare for an election. On election night, WinEDS accumulates the results from the results cartridges and provide reports to the jurisdiction. The Election Management System assists a jurisdiction in managing the election workflow, from ballot definition to accumulation and reporting of results. WinEDS is not Internet based.

[15] On an audio-machine, the technician uses headphones, activates the machine and verbally votes.

The warehouse that stores the voting machines in Ocean County measures approximately 35,000 square feet. The offices and storage area are on one floor. A mezzanine above the first floor is used for record storage. The building is locked at all times and is protected by an alarm system with glass break sensors, motion detectors, contact point sensors and pressure sensors. Clayton, Zimmerman and two chief technicians have keys to the building. Other staff must ring a bell to gain access. Upon entry, each staff member signs in using a time card system. The same procedure is required on departure.[16] According to Clayton, there has never been a break-in.

To protect against inappropriate access to the voting machines, two keys are tagged and assigned to each machine. One key opens the front and back doors and one key activates a poll switch. The keys are placed in an envelope and duplicate keys are maintained in one of eight locked key cabinets at the Voting Technology Center. According to Clayton, a key to a voting machine has never been lost.

At trial, an AVC used in the June 2008 Presidential primary in Ocean County was brought to the courthouse for demonstration purposes. Clayton explained and physically demonstrated the set-up diagnostic procedures for each machine for each election cycle.[17] On election night, the board worker opens the back of the machine, opens the front of the machine and privacy panel, assembles and places the privacy curtain on the front of the machine, the emergency ballot box is removed, the operator panel is detached and the power switch is turned on. Once the power is activated, the display window automatically reads the set-up diagnostics and generates a zero proof.

When the print maintenance log from the operator panel is activated, the maintenance log provides a summary of when the machine was reset the last time, the maintenance history and the last time it was turned on and off. The operator panel prompts the technician through each step of the set-up diagnostic process. Once the maintenance report begins to print, the operator panel then prompts the

[16] To gain access, visitors must ring a bell. Once admitted, visitors are required to sign a login sheet.

[17] Set-up diagnostics, conducted through the operator panel and through the use of menu-driven prompts, are displayed on the operator panel. The set-up diagnostics takes the technician through various steps to test each component, switch, light, buttons and write-in keyboard of the machine.

technician to complete the rest of the process. Next, the "cast vote" button is tested to ensure the light is working properly. The write-in keyboard, switches, lights, keys and other components are checked. Lastly, the buttons are pressed and the lights compared to the names on the ballot. Once the set-up diagnostics are completed, a tape of all the tests is printed from the machine.[18] The tape produced is then attached to the printer.

Next, the pre-accuracy and logic test ("Pre-LAT") is performed.[19] Pre-LAT includes examining the protective counter number that displays the number of total votes cast on the machine in its lifetime. The first step requires the technician to insert the key to open the polls. The operator panel displays "election verification report," and then begins to print the Pre-LAT zero proof report. Zero proof establishes that there are no votes in memory. Once the zero proof report is printed, the technician tests the switches.

Ocean County, comprised of thirty-three towns, prepares and prints thirty-three different ballot styles. Instead of manual Pre-LAT tests, the County uses simulation cartridges to conduct Pre-LAT testing. The simulation program is available and generated through WinEDS. Clayton writes a script for each mock election to determine the number of votes to be cast for each candidate or public question. The script is based upon the switch positions that are used for the election. The vote totals vary from election to election and range between sixty and one hundred votes being placed on the machine, typically in a pyramid format. The script is entered into the vote simulation module that is in the WinEDS program, and then loaded onto the vote simulator cartridge.

On direct-examination, Clayton testified:

> [e]ssentially in WinEDS there's a module that we can prepare a script to test the various candidates' positions and give them any number of votes. That script is then loaded onto a simulation cartridge that is inserted at the same time the results cartridge is in Pre-LAT. Basically that allows us to give any number of votes to any number of candidates.

---

[18] The maintenance diagnostic test is also done regularly for routine maintenance.

[19] In essence, Pre-LAT is a "mock" election in which votes are cast for candidates to test the switch positions and to verify votes cast. Pre-LAT is performed at the warehouse.

[Tr. 8:10-16, Mar. 3, 2009.]

After Pre-LAT, the technician closes the polls by turning the key to the "polls closed" mode. A beep sounds and Pre-LAT results begin to print. The results tape will disclose the public counter total and the protective counter number. The protective counter is a record of how many votes have been cast on the machine in its lifetime to that point. The public counter is the number of votes that have been cast for a particular election. The numbers are recorded on the envelope that accompanies each machine.

Clayton testified that, depending on the size of the election, the time between Pre-LAT and the election varies.[20] and may occur up to two or three weeks before the election. Since 1997, Ocean County has maintained all of the tapes obtained from set-up diagnostics and Pre-LAT.

Clayton described three strap seals (green, yellow and gray) used for each machine. For each seal, the serial number is recorded on the key envelope for each machine, the envelope is given to the board worker and a copy is maintained at the warehouse. The gray strap seal is applied after Pre-LAT, when a results cartridge is placed in the machine before the election. At the end of the evening, when the board worker closes the polls, the gray seal is broken and the results cartridge is removed. After an election, once the results cartridge is removed, a yellow strap seal is used to seal the cartridge port. This seal precludes a results cartridge from being inserted after the results cartridge has been removed. There is also a green seal that seals the emergency ballot box.[21]

The server is located in the Administration Building in the Information Technology Department. The laptops are locked at the warehouse and are used only for election matters. While there is no written protocol, Clayton represented that laptops are never connected to the Internet.

Voting machines are transported by trucks rented from Budget Truck Rental. Deliveries are made to over 300 polling places by staff members and part-time seasonal employees. Each truck delivers between thirty-two and forty-eight machines per day, with one Republican and one Democratic staff

[20] The time may occur up to two or three weeks before the election.
[21] As will be noted later in this opinion, the State has implemented new standardized seals for voting machines.

member assigned to each truck. The delivery process begins Monday, eight days before the election. If an election is for a single town or school board, the delivery is closer in time to the day of the election.

At the time of delivery, there is no one assigned to accept or sign a receipt to verify delivery. The retrieval process is exactly the same. It takes approximately five working days to return all of the machines to the warehouse. In response to a question voting machine deliveries, Clayton testified:

> [y]es, the way that we work the delivery of voting machines, all of our voting machines are bar coded. We have a bar code scanner so that the night before the delivery process begins. I provide routes to each of my technician teams. They will line up their voting machines in sequential order in their delivery order. The following morning when they're going to begin the delivery of the machines, as they're loaded onto the truck they're scanned - - the bar code is scanned signifying for our records that the voting machine has left our building.
>
> [Tr. 35:4-14.]

After the election, board workers bring the paperwork from the polling locations to the Municipal Clerks. At the Offices of the Municipal Clerks, the results cartridges are placed in cartridge readers and the results are downloaded into WinEDS enabled laptops. The results are transmitted remotely to the County server with the assistance of a staff member from the Board. Once received by the Municipal Clerks, staff members bring the paperwork to the Board's main office. After the results cartridges are downloaded and the results are transmitted to the server, the results cartridges are also returned to the Board. Once the election is certified, the results cartridges are returned to the warehouse.

Clayton testified that after an election, seal serial numbers and the tamper evident labels are inspected:

> [w]hat I'll do is make photocopies of all the seal numbers, assign them to the technician. Your job today is to compare the seal numbers the machine went out with to what the machine is returned back, visually inspect to see if any of the tamper evident labels show any type of wear or the security screw caps have in any way been tampered with, scratched, beat up, whatever.
>
> [Tr. 68:8-15.]

In response to questioning, Clayton noted:

QUESTION: In your capacity as a voting machine supervisor, have you personally ever observed any evidence of tampering of a voting machine after an election?

ANSWER: No.

QUESTION: You've never personally observed any broken seals or damaged screw caps?

ANSWER: No.

[Tr. 75:9-16.]

Clayton testified that after the February 2008 primary, an option switch problem was identified on one of the machines.[22] According to Clayton, Sequoia described the problem as one of poll worker error. To remedy the problem, Sequoia designed and provided plastic shields to place on the operator panels, in the future, to prevent board workers from pushing the wrong buttons. According to Clayton, no problems have occurred since that time.

Sequoia provides a customer service manual that describes a series of semi-annual maintenance diagnostics.[23] Ocean County conducts these tests quarterly and undertakes any necessary repairs. Four AA batteries are located on the central processing unit ("CPU"). A 12-volt battery, located on the bottom of the machine, provides emergency power during the day. The batteries are charged for 48 hours each month.

Clayton acknowledged the following: (1) the State has provided no training in seals or seal-tampering detection; (2) read-only memory ("ROM") chips can be removed from the DRE motherboard if someone has access to the back of the machine; (3) while ROM chips have serial numbers, staff does

[22] On February 5, 2008, for the Presidential primary, a difference surfaced between the numbers of votes cast for a primary candidate and the corresponding party turnout numbers. On the back of the machine there is a rectangular plate with twelve buttons, six on one side and six on the other side. When the machine is programmed for an election, the necessary number of buttons are sequenced and activated. In a primary election, one of the numbers is designated to be Democratic, and another is designated to be Republican. Before voting, each voter receives a Voting Authority slip. The slip identifies each voter as either a Republican or Democrat. Based on that slip, the poll worker presses the appropriate button on the DRE to trigger either the Republican or Democratic ballot.

[23] Maintenance diagnostics is performed on the AVC between elections, when no ballot or vote data is resident.

not maintain a record of the serial numbers; (4) not all protocols and procedures are memorialized in writing; and (5) there are no written policies for storing and securing the voting machines at the polling places.

4. ELISA GENTILE (WITNESS FOR THE PLAINTIFFS)

Elisa Gentile ("Gentile") is a high school graduate. For the past twenty years, Gentile has worked for the Hudson County Superintendent of Elections. Initially hired as a mechanic trainee, she was quickly promoted to warehouse assistant manager. Since 1998, she has held the title of Voting Machine Warehouse Supervisor. In 2004, when the County purchased the AVC, Gentile attended a comprehensive one-week technical training program offered by Sequoia. Gentile has also attended two WinEDS classes, provided by Sequoia.

Gentile supervises three permanent warehouse employees and is responsible for maintaining the voting machines, preparing the voting machines for upcoming elections and arranging for the transportation of the voting machines to and from polling places. General maintenance includes charging the 12-volt battery and four AA batteries in the voting machines every six to eight weeks. While charging the 12-volt battery does not require removal of any part of the machine, replacing the four AA batteries requires removal of the CPU cover. To verify the batteries are charged and working, staff then press button B2 on the operator panel located on the side of the machine. When the battery test report is complete a tape is printed and reviewed by staff.

The AVC is also equipped with a "set-up diagnostics" test feature. Once the set-up diagnostics is completed, the election ballot information is loaded from the WinEDS enabled computer onto a results cartridge. Gentile is the only person authorized to prepare the results cartridges and audio-cartridges. To transfer the information from the WinEDS enabled computer to the results cartridge, the results cartridge is placed into a cartridge reader and the information is then downloaded (commonly referred to as "burning") onto the results cartridge.

Pre-LAT is conducted once the ballot information is downloaded onto a results cartridge and the cartridge is placed into the voting machine. While some counties utilize in-house staff to conduct Pre-

LAT, Election Graphics ("EG"), a third-party consultant, is under contract to conduct Pre-LAT in Hudson County. The EG team consists of the same three to four team members for each election who are normally on site for two days. As part of Pre-LAT, EG members cast one vote for each candidate for each contest and one vote for each public question. After each vote is cast, the panel or write-in keyboard is viewed to verify that the name of the candidate, or the public question, corresponds to the button that was activated. The audio kit is also engaged to verify accuracy.

When Pre-LAT is completed, the results tape is printed to verify that the vote totals compare with the votes cast. If the results are satisfactory, a plastic seal is placed in each results cartridge. Generally, set-up diagnostics and Pre-LAT occur over a two-week window prior to the election.

In Hudson County there are 600 voting machines and approximately 245 polling places. Voting machines are placed in schools, firehouses, senior citizen centers, apartments and occasionally storefronts. A private moving company transports the machines to and from each polling place. The moving company, the vendor for over twenty years, typically assigns the same workers. Members of the warehouse do not accompany the movers during the transportation of the machines. Due to the large number of machines, some machines are left at polling places for up to one week. Upon arrival at the polling place, the machines are left without any signature required. After the election, over a period of approximately one week, the machines are returned to the warehouse.

Keys and duplicate keys for the voting machines are maintained in locked cabinets in Gentile's office. After Pre-LAT, Gentile and staff members lock the back door of each DRE. Gentile then collects the keys and places them in an envelope. The results cartridges are kept in the computer room, except when maintained in a locked room for the impoundment period after an election.

The voting machines are located on the second and third floors of a 30,000 to 40,000 square foot warehouse. Three hundred machines are stored on the second floor and three hundred machines are stored on the third floor. The building, rented by the County, is equipped with an alarm system that includes eye beam sensors and motion detectors. Describing the system, Gentile noted that crossing the eye beam or any motion in the warehouse will trigger the alarm system. In addition to the sensors and motion

detectors, each access door of the warehouse and the three parts of the warehouse floor are alarmed. To distinguish between who goes in and out, each staff member has a unique four-digit security code to gain access to the building. The office is open during the day Monday through Friday. There are no security cameras or security guards.

In response to the question whether Gentile agreed with the State's expert, Professor Andrew Appel's ("Appel") conclusion, that chips can be removed from the back of the motherboard, she responded:

> [i]f we remove the chip, a warning comes up that says check some chip change when we make a chip change, or we take out a chip. So, it can be removed, yes, but - - Does it go detected? I think it does with us at our level. When we have to remove a chip and change, we get notice at the printout that says the chip has been changed.
>
> [Tr. 63:21-64:4, Feb. 23, 2009.]

In response to questions regarding background checks for staff members or third party vendors, Gentile was not aware of any specific policy.

5. DARYL MAHONEY (WITNESS FOR PLAINTIFF)

Daryl Mahoney ("Mahoney"), a high school graduate, was hired by Bergen County in 1993 as a voting machine mechanic. In 1995, Mahoney was promoted to chief mechanic. Currently, as Assistant Director of Voting Machines, Mahoney oversees the operation of the voting machine warehouse. Mahoney supervises ten full-time employees.[24] Shortly before, during, and after an election, County employees are assigned from the main office to provide assistance. Mahoney has never taken any courses in computer programming, software, engineering, or security.

The County owns a one story building that houses 1,200 voting machines. The building is equipped with an alarm system that is deactivated when the first person enters the building in the morning. There are no security personnel on site. To gain access, employees use a code to disarm the alarm and a separate code to unlock the door to enter the facility. Each employee has a unique four-digit

[24] Mahoney is not aware of any policy that requires newly hired employees to undergo criminal background investigations.

code for the alarm and a unique three-digit code to gain access to the building. The 1,200 voting machines are organized alphabetically in three rows. The top of each voting machine identifies the town and district. Each machine has its own key attached to the machine.

The eight mechanics, including Mahoney, maintain and repair the voting machines. While staff performs set-up diagnostics and Pre-LAT for each voting machine, the County is under contract with Sequoia to download the ballot information. The County uses seven laptop computers to prepare the voting machines for an election. All of the laptops are stored at the warehouse. Approximately one month prior to the election, Joseph McIntire ("McIntire"), a Sequoia representative, downloads the ballot information onto each WinEDS enabled laptop using a jump drive.

In response to questions regarding connection of the laptops to the Internet, Mahoney stated:

> [t]hey're not connected to the Internet in any way. What we do is we have card readers that are attached to the laptops and the information is then loaded to the cartridges, put in a cartridge holder, along with the audio cartridge, and it's then put on the back table for the mechanic to come and pick up the cartridges and the ballots that are on the back table and set the machines up.
>
> QUESTION: You've said that they weren't connected to the Internet in anyway?
>
> ANSWER: Right.
>
> [Tr. 1, 111:7-19.][25]

The results cartridges are stored in locked cabinets, organized by town name, in cases that hold between fifteen and twenty cartridges. Once the ballot information is downloaded, cartridge readers are attached to the laptops and Mahoney personally downloads the election information from the laptop onto each results cartridge. Once the transfer is made, the results cartridges are placed on a table for the mechanics to place into the voting machines.[26]

---

[25] The two days of testimony are identified as follows: Tr. 1 (February 23, 2009) and Tr. 2 (February 24, 2009).

[26] If the machine has an audio-kit, an audio-cartridge will also be placed in the machine.

After the cartridges are placed in the voting machines, staff performs set-up diagnostics and Pre-LAT to verify that the voting machines accurately record votes. First, each button on the machine is checked to verify that the ballot face of the machine matches the ballot information on the cartridge. Staff then casts at least one vote for each candidate and public question. The results tape is then printed and the votes recorded are compared with the number cast. Once concluded, a certification is signed to verify the machine is prepared for the election.

In response to questions regarding software upgrades, Mahoney recalled one occasion in Bergen County when EG, contracted with by the County, upgraded the AVC voting machines form Version 5 to Version 9.00H. During the three to four weeks that EG team members were on site, the team was not suprevised.

A third-party vendor, also under contract with the County, transports the voting machines to and from the polling places. As long as Mahoney has been employed by the County, the same company has been under contract. Given the large number of machines, coupled with limited drivers and trucks, many voting machines are delivered to the polling places up to two weeks before the election. Once delivered, the County does not provide security at the polling locations.

After an election, poll workers open the back doors of the machines, remove the results cartridges, close the poll switches on the machines and print the results. Then, each poll worker breaks the seal holding the results cartridge and removes the results cartridge. After signing the paperwork, the results cartridges are transported to the Municipal Clerk's office by the head poll workers. Once the information is tabulated at the Municipal Clerk's office, the results cartridges are transported to the County Clerk's office. After the election is certified, mechanics retrieve the results cartridges from the County Clerk's office and return them to the warehouse.

Mahoney has served as a member of the Title 19 Election Committee (the "Committee" or "Title 19 Committee") for approximately six years. N.J.S.A. 19:48-2. In response to questions regarding updates, Mahoney recalled software upgrades presented to the Committee sometime in 2005 and

September 2006. Mahoney testified that upgrades/modifications that do not impair the accuracy or efficiency of the voting system do not require full recertification. N.J.S.A. 19:53A-4.

Describing his role on the Committee, Mahoney testified, "mine is the real world use of the voting machines." Tr. 2, 25:6-5. Regarding one of the other members, John Fleming ("Fleming"), Mahoney stated, "as far as the computer upgrades and stuff, that's Mr. Fleming's area." Tr. 2, 25:5-6. Mahoney testified the Chair, Richard Woodbridge, Esq. ("Woodbridge"), a patent attorney, prepares a draft report after each examination. Once the report is reviewed by the Committee and finalized by Woodbridge, the report and recommendation is sent to the Secretary of State. N.J.S.A. 19:48-2.

6. PAULA SOLLAMI-COVELLO (WITNESS FOR PLAINTIFFS)

Paula Sollami-Covello, the Clerk in Mercer County, supervises thirty-seven employees. Two of the employees are permanently assigned to election duties. The Election Supervisor, who reports to the Clerk, is responsible for handling the election process. This includes: (1) placing advertisements in newspapers for civilian, overseas and military mail-in ballots; (2) arranging for the printing of ballots; (3) accepting applications for mail-in ballots; (4) issuing mail-in ballots to voters; (5) counting the results cartridges; and (6) verifying the votes cast on the results cartridges on election night.

Mercer County owns 600 voting machines. On election night, after the polls are closed, each results cartridge is sealed in a canvas bag. The tape printout and numbered plastic seal is placed in the pouch on the front of each bag. At the polls, board workers sign and collect all of the paperwork. The results cartridges are then transported to the Offices of the respective Municipal Clerks. On election night, representatives from the Clerk's office retrieve the results cartridges and transport them to the Clerk's office. Each results cartridge is held by the Clerk's office until the election is certified. On election night, several election officials from the County are responsible for placing each results cartridge into a cartridge reader that is connected to a WinEDS enabled computer. Once inserted into the cartridge reader, the numbers appear on the computer screen and the votes are tallied.

After the votes are tallied and the results posted, the Clerk has a period of time to certify the election results. As part of the verification process, the printout tape from each machine is compared

against each results cartridge. Until the results are certified, the results cartridges are kept secured in the Clerk's office. Once certified, the results cartridges are returned to the warehouse. At the warehouse, the results cartridges are cleared and ready to be reused.

In the February 5, 2008 primary election, thirty machines disclosed a total tally that was off by one to two votes. For example, one case disclosed twenty-nine votes for a candidate for the Democratic Party when the registration records disclosed thirty Democratic voters.[27] As a result, the Election Supervisor prepared a report to memorialize the discrepancy.[28] Clerks and other election officials were notified that the problem, referred to as the "option switch bug," occurred as the result of poll worker error.

7. JOANNE RAJOPPI (WITNESS FOR THE PLAINTIFFS)

Since 1996, Joanne Rajoppi ("Rajoppi") has served as the Union County Clerk. Current member and past President of the Constitutional Officers' Association of New Jersey, Rajoppi is also the Director of the Clerks' Division of the International Association of Clerks, Records, Election Officials, and Treasurers.

Rajoppi described the procedures before, during and after an election. Before the election, Rajoppi designs the ballot for each town. Once the ballot definition is completed, the printer produces a ballot on a large piece of paper for each voting machine. The programmer at the warehouse then inputs data for candidates that correspond to the switch positions located on the ballot.

While the Clerk performs many pre-election duties, Rajoppi testified "at the close of polls, that's when our real work begins." [29] Tr.1, 40:24-25. After the close of the polls, board workers transport the results cartridges to one of four satellite offices. The four satellite offices include three Municipal Clerks' offices and the voting machine warehouse. For a municipality that is not a satellite office, a sheriff's

[27] The tape indicates the total number of voters that voted on that machine.

[28] While the party tallies were off, the actual votes cast for each candidate were correct.

[29] The two days of testimony are identified as follows: Tr.1 (2/26/2009) and Tr.2 (2/29/2009).

officer transports the results cartridges to one of the satellite offices. Each satellite office is equipped with cartridge readers and WinEDS enabled computers. According to Rajoppi, the laptops are not used for any purpose other than the elections.

At the satellite office, the results cartridge is inserted into a cartridge reader and connected to a WinEDS enabled laptop computer which then downloads the results onto the computer. Rajoppi provides an Information Technology professional at each satellite location. According to Rajoppi, the results from the satellite offices are then transmitted, in an E-mail format, through a high-speed dedicated T1 line to the Clerk's office.

As election totals are received from satellite offices the results are tabulated. After the results cartridges are read at the satellite offices, sheriff's officers transport the results cartridges to the Clerk's office where the unofficial election results are announced. The results cartridges remain at the Clerk's office until the election is certified. The day after the election, the verification process begins.[30] This process includes comparing the paper results tapes from each voting machine to the data on the summary reports. The results tape lists individual candidate totals from a given district and, in a primary election, identifies the turnout total for each party.

In response to the question, whether she believes the results tape is an "independent audit of the voter's intent," Rajoppi answered, "I do." Tr. 1, 160:4-18.

Rajoppi testified that since 1998 the AVC has been used without incident. On February 5, 2008, however, a difference surfaced between the number of votes cast for a primary candidate and the corresponding party turnout numbers. Rajoppi described the configuration of the buttons on the voting machine to explain what occurred. For example, in this election, button number six was assigned as Democratic and button twelve was assigned as Republican. Therefore, for a voter with a Democratic ticket, the poll worker is instructed to press the Democratic switch and button six to activate the machine. The Democratic button is on the top right-hand side of the machine. For a voter with a Republican ticket,

[30] Since 2003, Union County has used optical scanners to count absentee, emergency, and provisional ballots.

the poll worker is instructed to press the Republican switch and button twelve to activate the machine. That button is on the top left-hand side of the machine.

To verify the results of an election, the Clerk compares the vote total data contained on the results tapes, including the Option Switch Totals, against the data on the summary reports to verify the numbers match. This procedure is performed for every election. In February 2008, the Option Switch totals disclosed that 55 Republicans and 170 Democratic voters had voted in that district. When the candidate totals were tallied, the number of authorized slips disclosed 57 Republicans and 168 Democrats.

The discrepancies were reported to the Attorney General's Office and Sequoia. As previously explained, Sequoia determined the discrepancy in the vote totals originated from an "option switch bug." To correct the problem, Sequoia designed a plastic shield, attached by Velcro, placed on the rectangular plate, to prevent a poll worker from pressing the wrong button.

Another discrepancy, present in the June 2008 primary occurred when a freeholder candidate had a "tilde," or accent, over the end of his last name. While the summary reports generated from the ballot cartridges did not include his name, the name did appear on the sample ballots, the machine face, the absentee report, the provisional report and on the precinct report. To address the situation, on election night, Sequoia deployed a technician to hand-edit the results of the election.[31]

On cross-examination, the State asked a series of questions regarding problems in prior elections:

> QUESTION: And my understanding from your testimony is that in those ten years, you compared the paper tape to the summary report, correct?
> ANSWER: That's right.
>
> QUESTION: And in those ten years, you never had a problem or discrepancy between what you found on the paper tape that was printed from the machine and was printed on the summary report.
>
> ANSWER: Yes, that's absolutely correct.
>
> [Tr.2, 140:13-21.]
>
> ***

[31] Rajoppi later learned WinEDS can be programmed to include a tilde on a candidate's name.

QUESTION: So, anyway, the results from the paper tape to the printout from the summary report matched exactly is that correct?

ANSWER: From what period of time?

QUESTION: From 1998 to 2008, before the February 2008 election correct?

ANSWER: For the Presidential Primary 2008 correct. Yes, it matched.

QUESTION: And you relied on those results to certify the election; is that correct?

ANSWER: Of course.

[Tr.1, 141:18-142:3.]

8 ROBERT GILES (WITNESS FOR THE STATE)

Robert Giles ("Giles") graduated college with a Bachelor of Art degree in Psychology. In 1995, Giles was hired as an investigator for the Ocean County Board of Elections and after eight months, became a voting machine technician. At the time, the County used optical scan voting machines. As a technician, Giles maintained voting machines, conducted Pre-LAT tests and coordinated the transportation of the voting machines to the polls. Less than one year later, Giles was promoted to Assistant Supervisor. The Board employed a staff of thirty-four, including investigators, clerical staff, and technicians. Since the County does not have a Superintendent, the Board handles all aspects of the election process.

After two and one half years as an Assistant Supervisor, Giles was elevated to one of two executive supervisor positions. In Ocean County, there is one Republican Executive Supervisor and one Democratic Executive Supervisor. In this position, Giles oversaw the day-to-day operation of the office which included: (1) the care and custody of voting machines; (2) voter registration; (3) assigning and monitoring polling places; and (4) the training and assignment of board workers. Giles held this position from 1999 to 2008.[32] In May 2008, Giles became the Director of the New Jersey Division of Elections

[32] Since 2005, Giles has taught a course in Basic Election Administration at Rutgers University.

("Director"), a position within the Office of the Secretary of State. Giles has no formal training in computer science, computer engineering, or computer security.

As Director, Giles: (1) receives petitions for State and Federal offices; (2) assists the Secretary in certifying results for State and Federal offices; (3) monitors compliance with the National Voter Registration Act of 1993, 42 U.S.C. 1973 (gg) et seq.; the Voter Accessibility Act for the Elderly and Handicapped Act of 1984, 42 U.S.C. 1973 (ee) – 1; the Uniform Overseas Residents Federal Election Absentee Voting Law, N.J.S.A. 19:59-1 et seq.; the Help America Voting Act, 42 U.S.C. 15301 et seq. ("HAVA"); and (4) receives governmental funds and assists in the allocation of same.

As Director, Giles also coordinates applications submitted by vendors for the certification or recertification of voting machines or equipment. When a vendor applies to the Secretary of State, Giles collects all of the materials, Independent Testing Laboratory ("ITA") reports,[33] schedules hearings and handles all administrative aspects of the application.

According to Giles, prior to November 2008 there was no state-wide security plan for voting machines. Instead, each County developed and implemented independent security measures. In the summer of 2008, Giles met with the New Jersey Association of Election Officials, Voting Machine Subcommittee, to develop statewide uniform security standards. For the November 2008 election, uniform security measures had been adopted and implemented in all twenty one counties.[34] As part of the changes, counties were instructed to record serial numbers and to maintain a record of the serial numbers. Also, as part of an overall security plan, the State purchased and distributed tamper-evident tape and multi-lock cable seals.

[33] ITA reports are from approved federal laboratories that have been certified under HAVA and relate to the performance of voting machines.

[34] Giles coordinated with Warren, Sussex, and Salem counties to address machines other than the AVC.

The State's current plan for future elections includes the use of smaller half-inch cup seals, high security padlocks and tamper-evident tape.[35] According to Giles, each seal will be imprinted with a serial number.

A modification or upgrade to a voting machine, depending on the type and extent of the change, may require the machine to undergo recertification. Giles acknowledged the absence of statewide standards or guidelines that govern: (1) re-certification standards; (2) storage of voting machines; (3) transportation of voting machines to and from polling locations; (4) training of board workers; (5) regulating laptops or computers used to transmit election information; (6) connecting laptops or computers to the Internet; (7) the number of votes to be cast during Pre-LAT; (8) inspection and examination of seals or locks before or after an election; (9) the storage of results cartridges; (10) procedures for recounts; and (11) security background checks for election staff, vendors or third party consultants.

In exploring seal options, Giles contacted two seal manufacturers: American Manufacturing and Casting and Brooks. While the State plans to purchase seals from Brooks, Giles acknowledged that, as of May 2009, the State had no written agreement with Brooks. According to Giles, the small cup seal is available with an imprinted three digit serial number.[36]

As part of the process of gathering information for new seals, Giles acknowledged that: (1) he has not consulted with independent voting machine or security experts; (2) no seal protocol has been developed or contemplated as part of the seal acquisition search; and (3) currently no inspection procedures exist for examining seals intended for use on the voting machines.

9. RICHARD WOODBRIDGE (WITNESS FOR THE STATE)

[35] Giles testified the State intends to use a backing to make it easier to put on and remove from the voting machine.

[36] Plaintiffs' expert witness, Dr. Glenn Johnston, Ph.D. testified that the small cup seal is not available with a serial number. Giles testified that, while the small cup seal with serial numbers is not available in the catalogue, it is available by special order from the manufacturer.

Woodbridge graduated from Princeton University in 1965 with a Bachelor of Science degree in Electrical Engineering, and in 1971 was awarded a J.D. degree, with honors, from George Washington University Law School. Admitted to the patent bar, Woodbridge practices patent and trademark law in Lawrenceville, New Jersey. Since 1982, Woodbridge has served on the Title 19 Committee, on and off, for twenty-seven years. For approximately the past ten to twelve years, he has served as Chair of the Committee.

Woodbridge explained the process when a vendor files an application to introduce a new voting machine or applies for recertification or approval of an upgrade/modification to an existing voting system. Prior to the hearing, the Committee receives materials from the vendor. The type and volume of materials varies depending on the type of application. The materials provided by the vendor include operating manuals, reports, certifications from other states and ITA reports and related materials.

The Committee does not certify voting machines. Instead, the Committee advises the Secretary of State as to whether the machine satisfies the statutory standards. N.J.S.A. 19:48-2. In addition to a documentary presentation, the application includes a demonstration of the machine by the vendor. In considering the application, the Committee examines each of the criteria set forth in N.J.S.A. 19:48-1 and N.J.S.A. 19:53A-3. Once the demonstration is completed, the hearing is open for public questions and comments.

According to Woodbridge, during a demonstration members oftentimes cast votes and examine machines under different scenarios. No decision is made the day of the hearing. Instead, to provide members of the public the opportunity to submit written materials and comment, the report is finalized only after the public comment period.

Woodbridge estimated that since 1998, the Committee has convened on approximately thirty-five occasions, reviewed approximately eight machines and considered several requests for modifications or upgrades. As Chair, Woodbridge prepares a draft report and circulates the report to the other two members. Once the report is finalized, it is then transmitted to the Secretary of State. In the past five

years, Woodbridge recalled two occasions when applications were denied and vendors were required to return to the Committee to provide additional information.

In reaching a decision, the Committee does not confer with outside consultants, review the source code or conduct independent research. While the Committee does not examine the software or review the source code independently, Woodbridge testified that the software is always tested in the context of the operation of the machine.

In response to questions regarding whether Wyle examines software, Woodbridge responded:

> [h]istorically, Wyle has looked at just the hardware. I understand that they have expanded into software. One of the issues that you run into is it's hard to draw a line between the two because the functioning of the machine that Wyle tests, for example, it might be a thermal test where they heat the thing up or cool it down. You can't do that without the software installed.
>
> So the test Wyle does by its own very nature and because you're dealing with an integrated system, does include how robust or un-robust the software would be. But I believe the recent Wyle reports have moved into the software area.
>
> [Tr. 43:12-24, Mar. 4. 2009.]

In response to a question as to whether the Committee independently tested the third-party software contained in the voting machine, Woodbridge responded, "we examine the software in the context of the operating voting machine." Tr. 54:14-16.

In 1987, the Committee considered recertification of the AVC. At the time, the report issued by the Committee included language that "a similar machine was alleged to have been previously approved by the Secretary of State. There are eight differences between the machine previously approved and the present one." Tr. 72:10-13. Responding to the question of whether Woodbridge had any recollection of examining previous machines or reports, Woodbridge testified, "I have no recollection today, no." Tr. 73:16-19. To clarify, he noted that "it may very well have been one of those periods of time when I was not on the Committee." Tr. 72:23-25.

On approximately five occasions, when considering an upgrade or modification, the Committee waived full recertification. Woodbrdige recalled one such occasion, March 4, 2005, when the Committee

reviewed the tabulation system used to tabulate votes cast on the AVC Edge and Advantage. Since Microsoft had discontinued and no longer supported this prior version and developed a new version to improve functionality, the Committee did not require full recertification and limited its inquiry to the software upgrade.[37] Again, on November 14, 2006, the Committee met to consider new functionality in the WinEDS system.[38] By unanimous consent, members again determined that full recertification was not required. N.J.S.A. 19:53A-4 and N.J.S.A. 19:53A-3.[39]

10. JOHN FLEMING (WITNESS FOR THE PLAINTIFFS)

Fleming graduated from Trenton State College with a Bachelor of Science degree in Psychology. Fleming has no formal education in electrical engineering, computer science, or programming, or in computer security. While Fleming is not familiar with computer languages, he has hands-on experience in a broad range of computer operating systems.[40]

Since 1988, Fleming has worked for the Attorney General's Office, in the Data Processing Unit, as a Management Improvement Specialist, a non-supervisory title. Over the past twenty years, Fleming has received training from software product vendors. Fleming installs software, maintains the computers systems, servers and networks, installs wiring, replaces switches, and installs and replaces routers and parts. He is familiar with different kinds of memory, deals with computer viruses on a daily basis, and sets up firewalls to prevent the infiltration of viruses to the computer network.

---

[37] At the March 4, 2005 public hearing representatives of Sequoia were present. The minutes also reflect that the Division of Election invited all of the State's election officials to attend; approximately fifteen attended. (Ex. P-48, p. 1.)

[38] The minutes reflect that representatives from Sequoia, election officials from nine counties, a reporter from the Newark Star Ledger, NJN Public Television and several members of the public attended. The introductory paragraph of the minutes reflect that "Sequoia and its equipment have appeared before the State Committee on at least five occasions since 2001 at which they sought and received certification for voting equipment." (Ex. P-48, p. 2.)

[39] When such device has been improved any improvement or change which does not impair its accuracy, efficiency or ability to meet such requirements, shall not require a re-examination or re-approval thereof.

[40] An operating system, i.e., Windows 2000, MSDOS or Windows XP, is what the base computer runs on and a computer language, i.e., "C" language, is typically what a program is applied in. Fleming does not write computer programs.

Fleming described his job as "keeping the computer systems running." Tr. 38:21, April 1, 2009.

Since 2001, Fleming has served on the Committee. During that time, he has received no training.

11. PROFESSOR ANDREW APPEL (WITNESS FOR PLAINTIFFS)

A. BACKGROUND

Appel graduated in 1981, with highest honors, from the Physics Department at Princeton University. In 1985, Appel was awarded a Ph.D in Computer Science from Carnegie Mellon University with a concentration on programming languages, compilers[41] and formal methods. He returned to Princeton University in 1986 to join the faculty and has served on the faculty of the Computer Science Department since that time. In 1995, he became a full professor. Between 1996 and 2005, he served as Associate Chair of the Department.[42] Appel teaches courses in software engineering, programming languages, and election machinery. Election machinery includes voting machines, political parties, and the machinery of election administration by public officials.

Appel is a member of Princeton's Center for Information Technology Policy, an interdisciplinary center that brings together the fields of Computer Science and Public Policy. The Center is affiliated with the Woodrow Wilson School and is a joint venture between the Engineering School and the Woodrow Wilson School. The Computer Science Department at Princeton is part of the Engineering School.

Currently, his research ranges from the theoretical aspects of computer security that overlap with programming languages and formal methods, to the very practical aspects of computer security that relate to securing enterprise computer networks, physical security, security of memory systems and computer architecture. A Fellow of the Association of Computing Machinery, Appel is the recipient of several grants from the National Science Foundation for Scientific Research in programming languages, compilers and computer security, the Defense Advance Research Project Agency for research in computer security, the Advanced Research and Development Agency, the Air Force Office of Scientific Research for research in computer security, IBM, Microsoft and Sun Microsystems.

---

[41] Programs that translate source code into the executable programs that a machine uses.

[42] In April 2009, Appel was slated to become Chair, of the Computer Science Department in July 2009.

Appel is the author of ninety papers, eighty-three of which have been published in "peer review" journals, and two books on the topic of compilers. Appel has also contributed to chapters in several books and served as Editor-in-Chief of two professional journals.

While Appel has never held a position in election administration or had hands-on experience with election administration, he has published articles on: (1) the technology of voting machines; (2) the context in which voting machines are used; (3) technological developments in voting since 1850; (4) the reliability and accuracy of voting machines; and (5) individuals who wish to attack systems maliciously and the kinds of mechanisms and techniques available to them. None of the voting machine articles have been submitted for peer review or listed in his curriculum vitae.

The court qualified Appel as an expert witness in the areas of computer science, computer security, computer architecture and the AVC Version 9.00H. The sections that follow include information and recommendations offered during seven days of trial testimony as well as information and recommendations set forth in his expert report.[43]

B. SCIENTIFIC STUDIES AND PERSONAL OBSERVATIONS

To prepare as an expert witness Appel relied on voting machine documentation from Sequoia, scientific studies, electronic voting machine literature used in other states and countries, poll worker manuals, election administrative procedures, repair records and incident reports from election events. To observe voting machines before and after an election, Appel visited polling places as poll workers prepared for the opening and closing of the polls.

To prepare for the design of a vote-stealing program, prior to the summer of 2008, Appel compiled a team of experts to study WinEDS documentation, information disclosed during public hearings, ITA reports available to the public, and scientific literature produced by other computer scientists and security experts. According to Appel, this information described several classes of vulnerabilities, insecurities and inaccuracies in DREs.

---

[43] The several days of testimony are identified as follows: Tr. 1 (1/27/2009); Tr. 2 (1/28/2009); Tr. 3 (1/29/2009); Tr. 4 (2/4/2009); Tr. 5 (2/5/2009); Tr. 6 (2/9/2009); and Tr. 7 (4/14/2009).

The team focused on: (1) identifying potential vulnerabilities; (2) the possibility that a malicious person could install fraudulent firmware into the computer of the voting machine and cheat an election by causing votes to be changed even before the close of the polls; and (3) the option switch problem, identified in the Presidential primary election, on February 5, 2008. In this election, the number of votes recorded in the Republican primary was not consistent with the number of voters that the AVC reported as being enabled for that primary.

C. EXAMINATION OF AVC IN 2007 AND 2008

In 2007, Appel purchased five AVC Advantage machines over the Internet[44] and supervised a group of three Princeton University students. The students examined the hardware, software and firmware of the AVC Version 5 to estimate: (1) the time required to reverse engineer the firmware;[45] and (2) to disassemble one of the five AVC advantages into its separate components. The record reflects that it took two students, working full-time for one week, to reverse engineer twenty-percent of the firmware. After completing the examination, Appel directed the students to analyze each of the components and to set forth their findings. According to Appel, the difference between Version 5 and Version 9.00H is a software or firmware upgrade and that the hardware is practically identical, except for the daughterboard computer that implements the audio voting.

As a result of a court-ordered examination in the summer of 2008, a team of six scientists, selected by Appel, examined the AVC Version 9.00H voting machine. The examination included the hardware, source code, vendor manuals, documentation and firmware. In addition to Appel, who was one of the six members, the team consisted of Professor Brian W. Kernighan, tenured Computer Science Professor at Princeton who is one of the inventors of the "C" language (the language in which the AVC source code is written); Brian Cunningham, a Ph.D in Computer Science; Gang Tan, a Ph.D in Computer Science and an Assistant Professor of Computer Science at Boston College and Lehigh University; Maia

[44] The machines were purchased from an Internet auction site known as GovDeals.com, used by local, county, state and the federal government to auction surplus equipment.

[45] Reverse engineering is the process to recover source code from the firmware that is in the voting machines.

Ginsburg, who has a Master's Degree in Computer Science and is a lecturer in Computer Science at Princeton University; Christopher D. Richards, who has a Master's Degree in Computer Science and is working towards a Ph.D.; and Harri Hursti, an independent computer security consultant and voting machine expert. The team spent nearly seven days a week during the month of July 2008 examining the AVC, working between six to ten hours a day.

At NJSP Headquarters, the team had access to two AVC Version 9.00H machines. One of the machines had no tamper-evident seals and one had a small plastic strap seal. The team also: (1) examined a WinEDS enabled laptop computer provided by Union County; (2) studied WinEDS and the WinEDS user's manual; and (3) employed the WinEDS enabled laptop to prepare results cartridges to tabulate results.[46]

D. EXPERT REPORT

Following examination of the AVC Version 9.00H, Appel prepared an expert report. The report includes a narrative description of alleged insecurities and inaccuracies the team found in the AVC. In conjunction with the expert report, the team prepared videotapes on August 20 and 21, 2008. These videotapes, later transferred to four DVDs, recorded a complete test election cycle on the unmodified voting machine at the NJSP Headquarters. The DVDs demonstrate that once a vote-stealing program is installed, the data can be manipulated to change the results. During the taping lawyers for Sequoia, the State and plaintiffs were present.

E. FRAUDULENT FIRMWARE STEALS VOTES THROUGH ROM CHIPS

Appel described the motherboard of the AVC as a large circuit board that contains a Z80 microprocessor and other chips that serve as memory and input-output devices. One way to corrupt the firmware is to replace one of the four ROM chips. This could be achieved if: (1) an attacker purchased an AVC on the Internet and removed a ROM chip; (2) an attacker gained access to an unattended AVC; or (3) an insider decided to replace the ROM chip. This would occur if the computer program (firmware) in the AVC that translates the voters' selections into votes, and counts those votes, was replaced by

[46] Prior to July 2008, the team studied documentation by examining ITA reports and other sources.

fraudulent firmware. The team designed a vote-stealing program, burned it onto a ROM chip, and installed it into the AVC.

According to Appel, the program was designed to move votes from one candidate's total to another, while not changing the total number of votes cast.

> [a] computer takes its instructions in the form of "machine language," which is not convenient for humans to read and write. Computer programmers write programs in a human-readable format language called "source code," which is then translated by "build tools" such as a compiler into "machine language." A computer program, once installed in read-only memory ("ROM") inside a device such as a microwave oven or a voting machine, is often called "firmware."
>
> [Appel Expert Report, p. 14.]

The firmware for the motherboard is located on four ROM chips known as erasable programmable read-only memory ("EPROM"). While the chips fit snugly into sockets, each one can be pried off and removed.[47] According to Appel, installation of the fraudulent ROM chip is simple. First, the attacker picks the lock.[48] To access the ROM chip, an attacker then removes ten screws from the main circuit board cover (a rectangle of sheet metal approximately 17 x 14 inches), removes the ROM chip for approximately one minute to copy it, places the ROM chip back into the voting machine, puts the screws back in and walks away. According to Appel, this permits the machine to remain in its original state and provides the attacker with a copy of the firmware and the opportunity to take as many months as needed to analyze the firmware to know what to change to make it cheat.

Once an attacker replaces the fraudulent ROM chip and walks away, the firmware will switch votes from one candidate to another, according to an algorithm designed in the official election mode of the AVC. To avoid detection, the next time the computer is turned on or used in an election, the fraudulent firmware is already installed and will subtly misbehave during elections but not misbehave

---

[47] The motherboard also has random access memory ("RAM") to store data, such as the recorded votes and ballot definition. The motherboard contains RAM chips that will lose their memory when the power is turned off, and other RAM chips that do not lose memory when the power is turned off, due to the batteries that retain the vote data when the power is turned off.

[48] On average, defeating the lock takes about thirteen seconds using an ordinary Phillips screwdriver.

during Pre-LAT. The hacker does not necessarily need to check the ROM chip to make sure it's working. ROM chips are sold commercially on the Internet for less than $4 each. The ROM reader costs less than $150.

The team installed the fraudulent ROM chip and then video-taped a mock election. The Pre-LAT program was designed to change only the 20th vote, to illustrate a mechanism that fraudulent firmware can use to avoid detection.[49] Once the fraudulent chip is in the AVC and used in a legitimate election to produce fraudulent results, there is no method to retrieve the information that would record the voters' actual intent. As soon as the 20th vote has been cast, the data has already been altered and there is no copy of the true data left in the machine. It is gone forever. The AVC stores the votes recorded in four different ways, resulting in the fraudulent software changing the result totals in all four places.

Appel noted that the AVC does not test the ROM chip in any effective way to make sure that it is not fraudulent. Even if an effective test were present, it would be easy to remove because the legitimate firmware is being removed, and the fraudulent firmware would not include such a test:

> [w]hat we've seen in that printout is the total number of votes for each candidate. The file with these vote totals, one copy is stored in the results cartridge that comes out of the machine, and another copy is stored in memory that is mounted directly on the motherboard; two copies. And my fraudulent firmware made sure to alter both of these two copies consistently with each other.
>
> In addition, the AVC Advantage stores a list of valid images, that is, a record of the complete ballot cast by each individual voter. And so, this feature of the AVC Advantage is called by the name Audit Trail by its maker Sequoia. It's just a list of recorded ballot images that encodes, which candidates were voted for on this complete ballot. And one copy of this list of ballot images is kept on the results cartridge. Another copy is kept on the motherboard of the computer.
>
> And I designed my fraudulent addition to the firmware to change votes, not only in the vote totals, but in the recorded ballot images in each of those four places.
>
> [Tr. 2 111:17-112:13.]

[49] As described heretofore, Pre-LAT is a script prepared by the technician to run a mock election to verify the accuracy of the voting machine.

Appel noted that firmware is software stored in read-only computer memory that can retain its data even when power is not turned on. Therefore, unlike on a computer, where it is easy to install new software by simply pressing buttons, firmware is kept in a memory that is not so easily changeable. So, it's more firm or difficult to manipulate. In response to questions by the court, Appel noted that in the last thirty years, since the term "firmware" was introduced, its meaning has become a little bit blurred. This is because there is memory, known as flash memory, which retains data even when the power is turned off; similar to ROM. The flash memory, however, can be updated without physically removing any components. Apparently, in the voting machine industry, computer programs stored in flash memory are often referred to as "firmware," even though they can be replaced without changing any physical components.

Appel testified that maintenance technicians routinely remove circuit board covers to replace the batteries. If so inclined, these technicians would have the opportunity to pull out ROM chips and copy them. Third party vendors and consultants may also have unsupervised access. According to Appel, creating a vote-stealing program to operate in the AVC requires only basic programming knowledge equivalent to a Bachelor's degree in Computer Science or Computer Engineering. He represented that approximately 25,000 Bachelor's degrees in Computer Science are awarded each year in the United States.

Appel testified that fraudulent voting machine firmware can be written to avoid detection by: (1) maintaining a correct public counter (how many voters cast votes on the machine); (2) not stealing too many votes; (3) not cheating in the Pre-LAT mode; (4) defending itself against "parallel testing";[50] (5) taking into account the "digital fingerprint" that is part of the AVC; (6) stealing votes in election after election without the attacker ever needing to give it further instructions; or (7) if requested, only stealing

[50] Parallel testing is a process to detect fraudulent firmware. The approach is predicated on using workers on the day of the election to vote on a machine set aside at the polling place to evaluate their reliability and accuracy.

votes that are specific to that election. Finally, the audit trail is not independent of the firmware. If that firmware is fraudulent, then the audit trail itself can be fraudulent.[51]

On cross-examination, Appel acknowledged the limitations of the ability of the vote-stealing program to cheat in future elections:

> QUESTION: Professor, in the video that was shown in court during your direct examination in which the results of the installation of the vote-stealing programs demonstrated, you stated that the machine can cheat in the next election and every election thereafter? Do you recall making that statement?
>
> ANSWER: Yes.
>
> QUESTION: But the statement is only true if the candidate you want to steal votes from is assigned to switch position H13 and the candidate you want to receive the stolen votes is assigned to switch position E13; correct?
>
> ANSWER: In the particular demonstration program that I did for the video, that's correct.
>
> QUESTION: So in a future election, if the candidate that this program was designed to help was assigned switch position H13, your program will steal votes from that candidate.
>
> ANSWER: This particular demonstration program would do that.
>
> QUESTION: What would happen if a candidate was assigned to H13 but no candidate was assigned to E13?
>
> ANSWER: Then my demonstration program would not change any votes.
>
> [Tr. 6, 45:15-46:13.]

On cross-examination, while Appel testified a vote-stealing program could be designed based on candidate's names, he did not design that program. With regard to the level of sophistication of the vote-stealing program created, Appel was questioned as follows:

> WITNESS: In my initial testing of the very first version of the vote-stealing program I made, I installed it into the voting machine and it didn't steal any votes.

---

[51] In all four of these electronic copies, the fraudulent firmware modified consistently with one another but inconsistently with the way the voters actually cast their votes.

QUESTION: And who worked with you in creating the vote-stealing program?

WITNESS: The main person that worked on this part of the investigation with me was Maia Ginsburg.

QUESTION: Was it just you and Miss Ginsburg who worked on the actual creation of the firm - - vote-stealing firmware?

WITNESS: Yes, I'm sure I discussed the process with whatever other members of my team were present that day.
QUESTION: And what is Miss Ginsburg's education?

WITNESS: She has a Master's degree in Computer Science.

QUESTION: And in your report you indicate that you purposely built a less sophisticated vote-stealing program; is that correct?

WITNESS: Yes.

QUESTION: But is it your testimony that you had the capability of creating something much more sophisticated?

WITNESS: Yes.

QUESTION: Have you ever done it? A vote-stealing program more sophisticated than the one you built for this litigation.

WITNESS: No.

QUESTION: So even with having the advantage of the source code and basically no pressure of being caught, you didn't create anything more sophisticated than a vote-stealing program that could switch positions?

WITNESS: The purpose of the vote - -

QUESTION: Just answer yes or no.

WITNESS: I did not.

[Tr. 6, 80:19-82:20.]

F. FRAUDULENT FIRMWARE INSIDE THE Z80 PROCESSOR

Appel testified an attacker could physically replace the main computer chip on the motherboard with a fraudulent chip that steals votes. The Z80 CPU reads the instruction from the program in the

firmware and executes the instructions. The Z80 is capable of executing a broad range of programs, from video games to chess-playing programs.

The AVC uses a Z80 microprocessor chip as its CPU. The CPU controls input and output and interprets the instructions. A computer is composed of several components, such as memory, input/output devices, and the CPU which interprets instructions from the memory and commands the input/output devices. Modern day computers may contain all these functions on one chip. In the mid-1970s, when the Z80 was designed, not all of the functions fit on the chip. That is why the AVC has so many chips on the circuit board.

Appel estimated it would take at least a month to develop a fraudulent chip to replace the Z80 using a field programmable gate array ("FPGA"). This chip is designed to allow one to load something like firmware to simulate other computer chips. Once created, the fake chip looks no different than the legitimate chip. The chip is commercially available for $13 per unit. According to Appel, someone with a Bachelor of Science degree in Computer Engineering should be able to easily simulate a Z80. Installing the fake chip onto the Z80 is similar to the process of downloading firmware onto the ROM chip. One would use a FPGA programmer device, plug it into a computer and download the program for the FPGA into the FPGA.

To replace the Z80 processor chip it must be unsoldered from the motherboard. Assuming one enters the proximity of a voting machine with an already fraudulent chip, it should take about ten minutes to do a careful job of de-soldering the legitimate chip, replacing it with the fake chip, and then re-soldering the fake chip. This is in addition to the approximately seven minutes that it takes to gain access to the interior of the DRE. According to Appel, once the fraudulent Z80 chip is installed, there is no way to detect that it is a fraudulent processor.

While Appel testified an attacker could create and install a fraudulent vote-stealing program onto a Z80, on cross-examination, he acknowledged the following: (1) neither he or any member of his team ever designed and installed a fraudulent vote-stealing Z80 processor chip; (2) there is no scientific

literature regarding creating Z80 processor chips for voting machines; and (3) neither Appel nor any one else has ever created a fraudulent Z80 processor chip that has gone undetected.

G. DAUGHTERBOARD & VIRUSES DISENFRANCHISE VOTERS

The AVC has an "audio-kit" containing its own computer that resides on a daughterboard inside the cabinet, separate from the main circuit board or motherboard. Since it contains its own computer, it is very susceptible to viruses. Firmware in the daughterboard operates the audio voting. Appel testified that the firmware can also be replaced on the daughterboard, and that fraudulent firmware can get into the audio ballot cartridge and copied onto the daughterboard. Unlike the motherboard firmware, the firmware of the daughterboard does not reside in ROM. It resides in "flash memory." The flash memory contains the election control program, as well as ballot definitions and other files. Unlike ROM, which cannot be modified without removing and replacing physical computer chips, flash memory can be written and rewritten by the software (or firmware) inside the computer.

Appel testified that storing firmware in writable flash memory creates the real possibility that an attacker could install fraudulent firmware without any physical change to the voting machine. This could be achieved by installing fraudulent firmware into the daughterboard through insertion of an ordinary audio-ballot cartridge into the slot in the daughterboard. "In fact, Appel did exactly that. The whole process takes just a minute or two. It is easier than replacing ROMs because no tools are needed at all." Appel Report, p. 58.

Appel testified that firmware in flash memory is inherently more vulnerable to fraudulent replacement, than firmware in ROM. The fact that the election program can write on the very memory that stores the election program is potentially very dangerous. Appel testified that this design of the daughterboard is in violation of the Federal Election Commission 2002 and 2005 Voting Standards.

In addition to installing fraudulent firmware in the daughterboard, Appel testified there is a very severe vulnerability to firmware viruses that propagate through audio-ballot cartridges. In this way, an attacker can install fraudulent firmware without having physical access to the voting machine. As noted by Appel:

> [a] computer virus is a program that can copy itself from one computer to another, either through computer networks or through removable media such as cartridges. In addition to merely copying itself, the virus may also have a payload that performs some malicious act, such as stealing money, making fraudulent financial transactions, forwarding spam e-mail, or stealing votes inside election firmware.
>
> [Appel Report, p. 59.]

On cross-examination, Appel acknowledged that infecting the daughterboard with fraudulent firmware will affect the motherboard in one of two ways: either by disabling the voting machine in the first place, or by communicating to the motherboard fraudulent votes from voters who cast their vote by audio. The State represented, in the February 2008 primary, only four people voted by way of audio.

H. VULNERABILITY OF WinEDS

According to Appel, an attacker can easily inject a virus into the WinEDS system that could infect all the AVC machines in a county or state. This occurs because viruses can easily propagate through WinEDS either from the Internet or through audio-ballot cartridges. A virus carried this way into the daughterboard can steal votes, cause machines to fail in targeted ways, and propagate itself both to the AVC voting machines and WinEds computers where votes are tabulated. Moreover, an anti-virus program provides no useful protection against a specialized vote-stealing virus.

Appel described how this would occur. First, prior to an election, a poll worker inserts an audio-ballot cartridge into the AVC to inform the computer how to pronounce the names of the candidates. The audio ballot cartridge is then placed in the metal audio ballot receptacle in the machine. The voter uses headphones and follows the instructions to select candidates. If there is fraudulent firmware on the audio-ballot cartridge, then the election worker will be unwittingly installing that firmware into the AVC.

Even if this vulnerability were fixed, another method of vulnerability still exists: (1) the virus might write fraudulent firmware onto the ballot cartridge in addition to the ballot data; (2) an election worker might not even know that the computer was misbehaving because computer viruses operate in a stealthy manner; (3) an honest election worker using a corrupted WinEDS computer could unwittingly

cause fraudulent firmware to be copied to the ballot cartridge; and (4) in the normal course of preparing the voting machine for an election, that cartridge would be installed into the DRE.

Appel described three ways in which fraudulent firmware could get onto the WinEDS machine. First, if a malicious individual had direct physical access just to the keyboard and USB ports of the WinEDS system, the individual could walk up to the machine and install fraudulent software. Second, if the WinEDS computer is connected to the Internet, vulnerabilities in the Microsoft Windows operating system can allow attackers to take over the machine or to install fraudulent software on the machine. The third way is by viral propagation of fraudulent firmware through the medium of the ballot cartridges. Therefore, a virus can propagate: (1) through the AVC to other AVC machines; (2) from AVC machines to WinEDS computers; (3) from WinEDS computers to other WinEDS computers; and (4) from WinEDS computers to AVC machines.

Election workers use WinEDS to prepare the ballot definitions and copy the audio files onto an audio-ballot cartridge. When information is transferred, the audio-ballot cartridges are placed in the voting machine. The machine is transported to the polling place, and after the election the cartridges are removed and transported to election headquarters. Election workers then use the WinEDS software to extract the election results and tabulate the results.

In his expert report, Appel explains that propagation occurs:

> (1) When an "infected" audio cartridge is inserted into an AVC, the virus propagates into the internal flash memory of the audio-kit (daughterboard).
>
> (2) After that time, the virus resides in the internal memory of the daughterboard. If any uninfected cartridge is later installed into that voting machine, the virus copies itself onto that cartridge. That cartridge is now infected.
>
> (3) When an infected audio-ballot cartridge is inserted into a WinEDS computer, the virus copies itself into the Microsoft Windows operating system on that computer.
>
> (4) After that time, when an uninfected cartridge is inserted into the WinEDS computer, the virus will copy itself into the cartridge, thus infecting the cartridge.

> (5) Also, while the virus resides on the WinEDS computer, it can copy itself onto other WinEDS computers on the same network.
>
> (6) Viruses can also infect the WinEDS computers when they are connected to the Internet and used for web browsing. I found that the Union County WinEDS computer had been used for a substantial amount of Internet surfing.
>
> [Appel Report, p. 61.]

Appel testified it is easy for an attacker to inject into the WinEDS system a virus that infects all the machines in a county.

Appel examined the WinEDS computer from Union County and concluded it had regularly and repeatedly been connected to the Internet. Thousands of Internet entries appeared in the log, spanning a period of years, including the days leading up to and including the primary election of February 5, 2008. Each file in the computer system is stamped with the date that it was last modified. The dates were available for each use of the Internet web browser.

The ramification of having a WinEDS computer accessible to the Internet is that security vulnerabilities in the Microsoft Windows Operating System can be exploited by malicious websites. Over the years, new security vulnerabilities in Microsoft's operating system are continually discovered, and Microsoft patches those vulnerabilities as fast as it can. Websites that may contain malicious programs have the potential to insert viruses onto the WinEDS enabled computer that is used to visit those websites, either in the operating system itself or in application software on that computer. The record reflects that all of the defendants' experts agreed with Appel's assessment that connecting an election-related computer to the Internet at any point is inappropriate.

Appel testified that computers in any given county are generally connected to each other through a network. That network may or may not be connected to the Internet. If that network is connected to the Internet, then the infection from the Internet of even one machine on that network can propagate to all of the other WinEDS machines in that county's network. Therefore, if an attacker designed a virus to propagate fraudulent firmware through audio-ballot cartridges to the daughterboard, the infection would propagate through any of the WinEDS computers in the county's network. The fraudulent firmware

spreads by a virus that enters the daughterboard and can change the votes of voters who vote by audio. Additionally, the daughterboard can disable the motherboard when the computer is first turned on. When the AVC is first turned on, the motherboard sends a message to the daughterboard. If there is no response, the motherboard crashes and restarts. This keeps happening, causing the AVC to not function properly.

According to Appel, to create a virus that propagates itself does not even require a Bachelor's degree in Computer Science. It is also easy to reverse engineer daughterboard firmware by using commercially available software. The process is similar to that used to reverse engineer firmware on the motherboard.

While Sequoia provides to customers the "Computer Infrastructure Hardening Guidelines" that describe the steps to assist clients in securing their information systems infrastructure, Appel testified that the document is long and complicated.

Appel concluded that WinEDS is highly vulnerable to tampering, and there is no simple way to make it invulnerable.

I. SOURCE CODE NOT NEEDED FOR VOTE-STEALING PROGRAM

The source code for the AVC version 9.00H was provided to the team. Appel described source code as the formal description of a computer algorithm in a form that is easy for humans - or at least human computer programmers - to read and write, but is also automatically translatable to the form in which the machine CPU can directly interpret it. According to Appel, the team found many instances of undesirable engineering practices in the source code that would make it more difficult, for even the machine designers, to determine whether it was adding up votes correctly.

While the source code makes it more convenient to create a fraudulent program, Appel testified this can be done without the source code, through reverse engineering by someone with a Bachelor's degree or experience in Computer Programming or Computer Science. This requires access to the firmware or machine code. When there is a copy of the executable machine code stored in the ROM chip, reverse engineering can be done to recover the source code or something functionally equivalent to it.

Using the five AVC machines purchased over the Internet, students from Princeton University used a commercially available reverse engineering tool to reverse engineer the Version 5 firmware back into source code. The students reversed engineered twenty percent of the code in several weeks.[52]

J. ACCESS TO THE AVC MACHINE

Because voting machines are left unattended for long periods of time in public places, access to the AVC is easy. Access may occur before the election when machines are delivered to polling places.[53] According to Appel, if access occurs after the election, the attacker is able to install fraudulent firmware to cheat in the next election and every subsequent election.

Appel testified that the lock on the cabinet is easy to defeat. The lock is an inexpensive five-tumbler lock that can be duplicated at a hardware store for less than $2. Appel Report, p. 30. Without the key, an inexperienced attacker can pick the lock by using lock-picking tools that are commercially available. Appel picked the lock in an average of 13.2 seconds. According to Appel, in many counties there are insufficient controls to ensure the proper chain of custody of the keys.

K. SEALS PROPOSED BY THE STATE

Before an election, the AVC machines are prepared by installing a results cartridge containing the ballot definition. This is done by employees of the Superintendent (or equivalent), or, in some counties, by a third party consultant. After a results cartridge is inserted into the metal cartridge receptacle, a plastic strap seal is inserted through the cartridge and receptacle slot on the AVC sheet metal. Each plastic strap seal is stamped with a serial number.

When the polls close, poll workers remove the results cartridges that now contain records of the votes cast. To remove a results cartridge, the poll worker is trained to cut the seal and record the serial number on the results report before signing the report. Once the serial number is recorded, the results

---

[52] AVC voting machines are readily available on the Internet. In early January 2007, a county in North Carolina advertised 136 machines for sale. There are government auction sites in which governmental agencies sell surplus equipment and any person is eligible to bid on and purchase the equipment. Appel Report, p. 39

[53] Delivery of the machines may occur weeks prior to the election.

cartridge, results report, and serial-numbered seal should be placed into a bag. The training manual also directs the poll workers to seal each bag with a serial-numbered tamper-evident seal. At that point, poll workers should transport the bag to county officials.

Upon receipt of the bag, the results cartridge is removed from the bag and placed in a cartridge reader to tabulate the results. Appel testified that: (1) a sample review of result report forms from the February 5, 2008 New Jersey primary, disclosed that only half (26) of the seals had a serial number recorded on the form; (2) when the seal is cut at the polling place, the AVC remains at the polling place for several days until it is transported back to the warehouse; (3) the audio-ballot cartridge has no seal; (4) the circuit board cover can be removed without removing the flexible plastic strap that holds the results cartridge; (5) counties order each batch of new seals starting from "0" (defeating the purpose of numbered and logged security seals); and (6) the seals can be defeated using inexpensive and low-tech methods.

In November 2008, the State provided Appel with three different physical security devices that were used in the November 2008 election. The first was a cup seal, referred to by Sequoia as a security screw cap.[54] The second was a wire cable seal to be installed through a hole in the circuit board cover and a corresponding hole in the circuit board enclosure to link the circuit board cover and the circuit board enclosure to the housing. The third security device was red pressure sensitive adhesive tape used to attach the circuit board cover to the cabinet of the AVC.

According to Appel, after examining the seals for a few hours, he removed the seals and, within seven minutes, re-installed the seals leaving no evidence of tampering. Appel testified that seal samples are readily available on the Internet.

In December 2008, Appel was advised the State intended to use new seals. On December 30, 2008, at a state facility in Hamilton Township, Giles demonstrated the placement of these new seals on a voting machine. The seals included a cup seal, a blue padlock device with a plastic padlock and metal hasp, and red pressure sensitive adhesive tape. Appel testified that he defeated each one, and on January

[54] There are ten screws that hold a circuit board cover to the AVC, and the cup seal is placed over one of these screws.

27, 2009, submitted a report on the three new seals. He did not record the length of time to defeat the newer seals.

In court, Appel demonstrated the defeat of each of the seals. These were not done on an actual voting machine. First, using a block of wood on a table, Appel began with a half-inch cup seal with no serial number. To achieve the defeat, Appel used a screwdriver, cold chisel with a tip grounded to a round profile, a pair of pliers and a hammer. He pried off the old base, damaged by the removal and replaced it with a new base. Second, the blue padlock is a plastic base with a metal hasp that keeps the large 14-inch by 17-inch circuit board metal cover in place. To defeat this seal, Appel created a wooden and steel device as a template and drilled two little holes into the padlock. To achieve this, he used a $1/16^{th}$ inch diameter drill bit. To release the metal spring holding the hasp in place, Appel made a steel cylinder about three inches long and 5/8 inch in diameter. Next, using a wrench, he released the base of the padlock from the hasp and re-installed the blue plastic padlock seal. After this was completed, the two holes were visible, albeit subtle with a little damage to the top of it.

On cross-examination, the State asked Appel to remove and reinstall the ROM chip, disassemble all of the parts, remove and reinstall all of the seals, and return the voting machine to its original position. The time to complete all of this was measured by a timer on the judge's bench. The timer was activated when the demonstration began and deactivated upon completion. The display on the timer disclosed a time of two hours and forty-five minutes. To the court's untrained eye, most of the seals appeared unaltered with a few showing minimal damage.

L. USER INTERFACE AND DESIGN OF THE AVC

Appel testified that the user interface, the physical and logical design of how the computer interacts with the voter, is flawed. He concluded:

> [t]he full-face buttons and lights design of the AVC user interface has inherent design weaknesses: it is unable to give certain kinds of feedback to the voter. In particular, really effective feedback about undervotes is difficult to achieve, and there is an inherent possibility for voter confusion about whether the machine is activated.

> However, even given that inherent limitation, Sequoia has made certain unavoidable design mistakes that greatly increase the risk that the intent of the voter will not be recorded. The behavior of the machine when not activated is inexcusable; pushing a button lights the green X's even when no vote is being recorded. The machine is too easily deactivated either inadvertently or surreptitiously before the voter has a chance to vote. And, there is a voter-privacy violation that could have been avoided with a better physical design.
>
> These flaws have the effect of disenfranchising voters, either inadvertently (with no malicious intent on the part of the poll workers) or on purpose. Thus, they compromise both the accuracy and the security of the AVC Advantage.
>
> [Appel Report, p. 87.]

Appel concluded that these alleged design flaws disenfranchise voters. He also testified regarding problems with the write-in vote procedures on the AVC. While for all the other buttons a voter may change their vote if there is an error, once the "enter" button is pressed for a write-in vote, the voter cannot change it before pressing the "cast vote" button.

M. THE AVC IS INSECURE

Appel testified vote data is not electronically authenticated, making it vulnerable to tampering. Sequoia represents, in its promotional literature, that AVC is using "cryptographic" means to guarantee authenticity, integrity, and confidentiality of votes. According to Appel, that is simply not true. Appel Report, p. 88. Cryptographic is an informal term for the standard phrase "digital signature." It is used to protect computer data so that accidental or deliberate modifications can be detected. In examining the source code, Appel found that:

> [t]here is no use of digital signatures or "cryptographic signatures" at all. There is not a single piece of data or firmware that is protected against deliberate fraud by the use of digital signatures.
>
> Hash functions are weaker than digital signatures – they can detect accidental data changes but not deliberate falsification. In the AVC no hash functions at all are used to protect actual vote data.
>
> Some of the hash functions used are even too weak to protect reliably against inadvertent data modifications.
>
> [Appel Report, p. 90.]

Appel concluded that any authentication the AVC performs is useless against deliberate fraud. When Appel examined an attack on vote data or firmware, either there was no authentication mechanism or he was easily able to defeat whatever mechanism was present. Appel also testified that the results cartridge used for transmitting the ballot definition to the AVC is easily manipulated. The results cartridge contains the ballot information as well as the votes cast. Appel wrote a program that runs on a computer and changes the votes inside the candidate-total files stored on the results cartridge.

The results cartridge contains the ballot definitions, including candidate names and contests and how they are positioned on the full-face ballot. In essence, it is a passive container of digital information, which can be plugged into a computer and its content changed. An attacker can achieve this before the election by changing the ballot definition. After the election, the attacker could fraudulently alter the outcome of an election by changing vote data in a results cartridge once the cartridge is removed from the AVC at the polling place, and before it is inserted into the WinEDS computer for tabulation. According to Appel, WinEDS cannot detect that the vote data has been altered.

When the polls closed, Appel observed results cartridges removed from voting machines and carried by poll workers to a table that also held the poll books. The results cartridges remained on the table while the poll workers completed their paperwork. Appel concluded it would be possible, at this point, for an attacker to gain access to the results cartridges and manipulate them.

Eventually, the results cartridges are placed into canvas bags by the poll workers and taken to a central location for tabulation. At any point during that time, someone with access to the results cartridge could use a computer to alter the data on the cartridge. To achieve this, one would only need a computer capable of plugging into the port in the results cartridge, as well as software installed on a computer that is designed to alter the vote data. WinEDS software could accomplish this.

According to Appel, there are several opportunities to manipulate the cartridge:

> by the poll worker who removes the cartridge from the machine, before bringing it to the table where the other poll workers witness putting it into the bag;

> By a poll worker at the table, while the other workers are busy with other tasks;
>
> By a person who transports the cartridge to county election officials for tabulation; and
>
> By a person who removes the cartridge from the bag before tabulating in WinEDS.
>
> [Appel Report, p. 91.]

As a result, "once the results cartridge leaves the voting machine, it is immediately susceptible to modification of vote data." Ibid.

First, "a cleverly designed ballot definition can cause a single button on the voter panel to add two votes for a candidate, or to have an invisible button add extra votes. The AVC does not thoroughly check the ballot definition data structure to make sure it is well-formed." Id. at 95.

Second, the mechanism for consolidating votes of several AVC machines in a precinct into one cartridge is insecure and subject to manipulation and fraud.

Third, wireless access to results cartridges opens avenues to manipulation. "Inexpensive and readily available technology would permit an attacker to make a fake audio-ballot cartridge that can be radio-controlled from several feet away." Id. at 99.

Fourth, a fraudulent intelligent results cartridge could steal votes. An undergraduate student of Electrical Engineering or Computer Science has the skill to accomplish this.

> This attack does not require any access to the internal circuitry of the AVC. To replace a results cartridge when the machine is turned off, at most requires picking the lock and defeating a seal. However, election insiders can insert fraudulent intelligent results cartridges into the election process without any access to the AVC. This can be done when results cartridges are being programmed with ballot definitions, when they are being read to extract results after an election, when they are stored in warehouses, when they are being manufactured, or at other points.
>
> [Id. at 102.]

N. COMPUTER PROGRAMMING ERRORS

One implication of the software problems is that bugs present in the software go undetected by Sequoia engineers, consultants, or outside agencies. According to Appel, if the software uses sloppy practices, it is harder for engineers who examine the software to determine if bugs are present, and these bugs could go undetected for many years. There are several types of bugs. A bug is a programming error, usually assumed to be inadvertent, that causes the program to malfunction in some way or to be vulnerable. A virus is a deliberately created piece of software. A ballot definition bug is a data file that has the names of the candidates, the offices, and the political parties laid out in a particular manner. It is feasible to develop ill-formed ballot definitions to manipulate an election and go undetected. One with ill intent could manipulate software in such a way to create two votes for a given candidate if one button is pushed. This could be achieved by manipulating the contents of the results cartridge prior to the election, or through a corrupted WinEDS.

Appel testified that computer programs should adhere to the best practices of software engineering. Regarding the source code in this case, he noted:

> I found that many of these – many instances of undesirable engineering practices in the source code that would make it somewhat more difficult for even the engineers who built it to determine whether it was correct or to get it to be correct. And by correct, I mean adding up the votes right, but also, being resistant to fraudulent manipulation and attackers.
>
> So, I found many instances of what I would characterize as sloppy engineering practices that I would think are inconsistent with an application in which the correctness and security of the program is of highest importance.
>
> [Tr. 3, 119:23-120:9.]

Later, in response to further questioning, he noted:

> [o]ne implication is that there could be bugs in the software that are present, but as yet undetected by Sequoia engineers or by others outside Sequoia who have examined the software. And to the extent that the software is unclear or makes use of these sloppy practices, it's harder for engineers, both those at Sequoia and those outside who examine the software, to determine if such bugs are present. Such bugs could go undetected for many years and show up.
>
> [Tr. 3, 121:19-122:2.]

The option switch bug surfaced in the February 2008 election. The results report printout was inconsistent with itself in that it reported more Republican votes than Republican voters. This happened in eight counties on approximately thirty-six machines. Appel noted that the presence of this bug is an indication that it slipped through: (1) Sequoia quality control; (2) the ITA that reviewed the software; and (3) state certification boards that approved the AVC for use.

In response to a question regarding what the result of the malicious use of the option switch bug would be, Appel responded:

> I actually don't believe it would be a very effective way of trying to cheat in elections because the anomaly appears on the printout. I think the significance of the options switch bug is not that it's a pathway to vote fraud in itself. It's an indication of the presence of bugs in the AVC Advantage software that slipped through all of the quality control processes, both at Sequoia and at ITA where they review that software and at state certification boards that accept the AVC Advantage for use.
>
> [Tr. 4, 55:6-15.]

Appel also described the ballot definition bug. He noted:

> there are certain kinds of ill-formed ballot definitions that one might use to try to manipulate elections, and those forms of ill formedness would not be detected by the AVC Advantage voting machine, and this would render the voting machine vulnerable to the effects of viruses that might infect WinEDS.
>
> [Tr. 4, 12:14-20.]

Appel testified that the abnormality is in the inability to detect the bug. Regarding the impact of human manipulation, the following colloquy is relevant:

> COURT: In the absence of that human manipulation, is there any bug in the ballot definition form?
>
> WITNESS: In the absence of ill-formed ballot definition the bug I'm talking about now is a bug in the detection of certain kinds of ill-formed ballot definitions. So, if the ballot definition is well formed, then the bug is latent and will not immediately cause an effect.
>
> QUESTION: Did you discover what actually caused the bug?
>
> WITNESS: I reviewed portions of the AVC Advantage source code for the purpose of checking for ill-formed ballot definitions in the cartridge, and I found that those checks were incomplete in some ways.

[Tr. 4, 11:23-12:16.]

Appel identified two different ways to manipulate elections because of incomplete checks for ballot definition validity: the two votes for one button and the use of a button not marked. He acknowledged, however, that this required the collusion of several people and was therefore not as severe a vulnerability as a ROM replacement, which did not require collusion. Another example of the failure to check for well-formed input is a buffer overrun. A buffer overrun error is a common kind of computer programming bug and means fraudulent firmware in the daughterboard can crash the motherboard firmware.

Finally, third party software is used on the AVC. Appel testified that software components, not designed and built by engineers at Sequoia, but introduced into the voting computer create the possibility for malicious people to corrupt elections by introducing fraudulent firmware in these other components. As a result, third-party software imported into a voting system has the real potential to infect that system with a vote-stealing software program by opening up additional pathways for installation of fraudulent firmware.

Appel concluded the AVC is not secure and is not entirely accurate. Most significantly, the insecurity of the AVC is not remediable by changes to the firmware. If the remedy is a change to the firmware, and the attacker removes the legitimate firmware and installs fraudulent firmware, then any remedy based on improving the firmware will not be effective in securing the AVC Advantage. In other words, the firmware could change the bugs, but security concerns about tampering remain.

O. UPDATES TO FIRMWARE

There have been many substantial firmware rewrites of the AVC since its introduction in 1980. The hardware, from 1984 to 2002, had just a Z80 (motherboard) computer. Since 2003, it also has a more powerful daughterboard computer. The Version 9.00H in New Jersey uses the daughterboard just for audio voting. In the Version 10 machine proposed for use in New Jersey, the daughterboard is the main processor. Between 1994 and 2003, the size of the firmware more than doubled. As a result, different

versions of the AVC mean significantly different voting machines that differ in their security, accuracy and reliability. Appel characterized the changes as substantial enough that they can be expected to affect or impair the accuracy, efficiency, or ability to meet the technical requirements imposed by Title 19.

In 2003, Sequoia added the audio-voting feature to accommodate disabled voters who are unable to use the full-face visual interface. This is a major change, because the 1976 vintage Z80 used in the 1980s design is insufficient to handle audio. As a result, Sequoia added an "audio kit," which contains a second processor to drive the headphones used by disabled voters, and a hand-held unit containing a third computer.

Appel's expert report includes a chart to demonstrate the changes made to the AVC firmware and how it differs substantially in functionality from year to year. Expert Report, p. 130. The chart, starting with Version 5.00 in 1994 and ending with Version 9.00H in 2005, includes three columns: (1) the version; (2) date; and (3) added features. Appel concluded that each version should have been separately examined for security and accuracy prior to approval. Appel Report, p. 132.

VERSION	DATE	ADDED FEATURES
5.00	1994	Multiple ballots
6.00	1995	Post-QAT
7.00	1996	Expanded option switches; early voting
8.00	1997	Dozens or hundreds of bug fixes minor changes
8.00A	1998	Mostly documentation changes
8.00B	1999	Bug fix
9.00	2003	FEC modification requests; audio voting
9.00C	2003	Bug fixes; updates to FEC coding standards
VERSION	**DATE**	**ADDED FEATURES**
9.00E	2003	

9.00G	2004	
9.00H	2005	Changes to audio voting and/or requirements

P. APPEL'S RESPONSE TO QUESTIONS RAISED BY EXPERTS

Appel rejected a recommendation by the State's expert, Michael Ian Shamos ("Shamos"), that a port could be installed to test the contents of the ROM without having to remove them from the circuit board of the voting machine. First, the port is not present on the AVC. Second, to add a port would require a redesign of the circuitry on the motherboard, and then prototypes of the motherboard would have to be tested and debugged. Third, the redesigned motherboard would have to be sent through the examination and certification process. Appel Report, p. 57. Finally, the process is too time consuming, expensive, and impractical.

In response to questions on cross-examination, Appel acknowledged: (1) absent user interface errors and if the AVC is not hacked, the internal computational errors are well under one percent; (2) the AVC compares favorably to other touch screen voting machines;[55] (3) the AVC provides adequate protection against over-voting (no studies were done to measure user interface errors); (4) if one plans to steal votes, the attacker would have to make sure the program steals the appropriate number of votes and install the program on enough machines to have an impact; (5) if the attacker is taking the trouble to construct fraudulent firmware and install it into voting machines, then a review of precinct-by-precinct vote data from past elections would be worthwhile; (6) more votes are going to be stored on the motherboard than on the daughterboard, i.e., in Bergen County during the February 5, 2008 primary election, only four people voted by way of audio; and (7) the daughterboard cannot cause the motherboard to change votes cast the normal way through the voter panel.

[55] The error rate for optical scan machines is one hundredth of one percent, or one tenth of one percent.

Appel rejected the notion that either parallel testing or checkpointing[56] was reliable in detecting fraudulent software. Instead, fraudulent software can be designed to defeat the protocol of both. According to Appel, parallel testing among experts in computer security is considered an inferior method of establishing the security of an election, as compared to software independence, such as a VVPAT or a precinct-count optical scan machine. Parallel testing is not a substitute for a VVPAT. Any given parallel test protocol can be defeated by a more sophisticated fraudulent program that will avoid cheating under the circumstances of that protocol. Appel concluded: (1) checkpointing is not a reliable means to detect fraudulent software; (2) it's not possible to do checkpointing on the AVC; and (3) it has never been tried.

Q. SOFTWARE INDEPENDENCE

In order to make the AVC more secure, Appel recommends that the State adopt Software Independence, a well-recognized principle among experts.[57] Since one cannot be sure what software is in a voting machine at any given time and one cannot be sure exactly how a given piece of software works, an independent source of verification is critical. If a voting system has software independence, results of an election can be trusted. This can be achieved through various forms of a VVPAT.

Appel testified that in 2006, the Technical Guidelines Development Committee ("TGDC") of the EAC adopted a resolution calling for software independence in the next generation of voting machines on the basis of definitions in a National Institute of Standards and Technology ("NIST") report. Appel Report, p. 51.

> A voting system is software independent if a previously undetected change or error in its software cannot cause an undetectable change or error in an election outcome. That is, the votes should be countable independent of the behavior of any computer software. This is because (1) software is so complex in general that it is not possible to be confident that it is adding the votes correctly, and (2) it is inherently

[56] Appel described checkpointing as similar in many ways to parallel testing. Rather than reserving a machine for an entire fourteen hour election day, the program can be designed to cast a certain number of votes on the machine at some point in the day, between other voters using the machines to actually cast votes.

[57] Software independence is premised on the notion that one should be able to count the votes in an election, independent of the need to rely on any particular piece of software.

> difficult or impossible to know what software is currently installed inside a voting machine or computer.
>
> [Ibid.][58]

According to Appel, twenty-two of the twenty-five election technology experts published in "Who's Who in Election Technology" agree that paperless DREs such as the AVC are unacceptable. Id. at 52. Computers may be used, but must be verifiable independently of the computer program. The only available technology that combines computer technology with software independence is the VVPAT. To verify the results, not every precinct must be recounted. Instead, a very small statistical sample of precincts or ballots needs to be audited. The New Jersey law passed in 2008 requires this kind of audit. Appel recommends that the Legislature implement immediately the 2008 law that provides for a VVPAT and statistical audit to protect the votes of New Jersey voters. Id. at 140.

There are three forms of VVPAT: (1) hand-counted ballots; (2) precinct-based optical scan ballots counted by computer; and (3) paper ballots automatically printed by DRE voting machines. According to Appel, computer security experts have come to a firm consensus that the most robust, reliable, and trustworthy form of software independence is the precinct-based optical scan machine. Appel shares this view based on articles in professional journals, news reports, and analyses by computer security voting experts who have examined voting machines and observed elections. Software independence ensures that the accuracy of the results can be guaranteed independent of the behavior of any particular piece of software.

On cross-examination, while Appel acknowledged that precinct-based optical scan voting machines can be hacked to miscount votes, he testified that a VVPAT is the best known method for achieving accuracy and security in balloting.

R. SUMMARY OF CONCLUSIONS BY APPEL

Based on seven days of testimony and the expert report submitted, Appel's most significant findings are listed as follows:

[58] The TGDC recommendation for software independence was not adopted.

(1) the AVC can be hacked to steal votes by replacing its firmware;

(2) the hack can be perpetrated by a person with only ordinary training in computer science;

(3) a person can easily gain access to voting machines to install this hack;

(4) once installed, the fraudulent firmware is practically impossible to detect; there is no paper audit trail; and all electronic records of the votes are under control of the firmware, which can manipulate them all simultaneously;

(5) once installed on a voting machine, the fraudulent firmware can steal votes in election after election without any additional effort;

(6) the AVC is vulnerable to hacks (fraudulent manipulations) in several different ways;

(7) some of these hacks take the form of viruses that can automatically propagate themselves from one voting machine to another;

(8) even when not hacked, the AVC (in its normal state) has design flaws that can cause votes to be lost, or cause voters to be given the wrong primary ballot to vote;

(9) even when not hacked, the AVC in its normal state has design flaws that encourage voter error and poll worker error and permit fraud;

(10) an ITA report is not an effective validation of the accuracy of the source code. While Wyle examined all of the motherboard firmware, it failed to examine all of the daughterboard firmware; and

(11) the overwhelming consensus of computer security experts is that the ITA is not effective in guaranteeing the security or evaluating the security of a voting machine.

After creating a fraudulent ROM, the legitimate chip on the motherboard can be replaced with the fraudulent chip. Additionally, the Z80, the central processing unit that masterminds the AVC, can be replaced by an imitation designed to steal votes. The daughterboard is more vulnerable to attack then the motherboard since the attacker can replace the firmware on the daughterboard through the audio-ballot cartridge stored in rewritable flash memory. Finally, as a result of a single WinEDS computer becoming infected with a virus from the Internet or a malicious act by an insider, every AVC in the county could become infected through the routine use of audio-ballot cartridges, without any further intervention by the attacker.

S. POINTS RAISED BY THE STATE ON CROSS-EXAMINATION

During cross-examination, the State established the following:

(1) prior to the installation of the fraudulent ROM on August 20, 2008, the AVC accurately counted the votes cast in the Pre-LAT and then accurately counted the votes in the official election mode;

(2) the AVC keeps in its internal memory a list of the ballot images of each ballot cast, a feature known as an audit trail. There is a command on the operator panel to produce a printed audit trail from the internal memory;

(3) the AVC has redundant storage of the same thing in four different locations;

(4) the fraudulent firmware, created by Appel, was election specific and would not produce the same fraudulent results in a subsequent election;

(5) the AVC provides adequate protection against over-voting;

(6) the attacker must have physical access to the AVC to install fraudulent firmware in the motherboard;

(7) the fraudulent firmware, designed by Appel, will work only if candidates are placed in specific switch positions;

(8) the fraudulent firmware, created by Appel, is not able to switch votes based on the candidate's name;

(9) an attacker would need source code or its functional equivalent through reverse engineering, to create a fraudulent vote-stealing program;

(10) two graduate students at Princeton University, who had received their Master's degrees and were studying for their Ph.D., reverse engineered approximately 20% of the firmware of the Version 5 AVC;

(11) it would take twice as long to reverse engineer Version 9:00H than Version 5;

(12) Appel has never designed fraudulent firmware that would modify the Z80 processor;

(13) Appel has never actually modified a Z80 processor chip;

(14) it would take at least a month to develop a fraudulent Z80 processor chip that would cheat in elections;

(15) Appel did not remove the Z80 chip from the circuit board on the voting machine;

(16) Appel has never installed a vote-stealing program on the inside of a fraudulent Z80;

(17) Appel did not design or implement a vote-stealing program that would work on the daughterboard;

(18) Appel never reverse engineered the daughterboard firmware;

(19) the option switch bug was a result of poll worker error when the machine was used in a manner inconsistent with the operator's manual;

(20) attack of the padlock seal left evidence of tampering due to the holes that were drilled in the top of the padlock seal;

(21) after the demonstration, the base of the cup seal was damaged;

(22) the courtroom demonstration of attacking the seals installed on the voting machine took over two hours;

(23) an attacker would need to change the legitimate ROM chip with fraudulent firmware in approximately 500 machines in order to have an impact on a statewide election;

(24) if an attacker realized the firmware had been updated after designing a vote-stealing program, the attacker would retreat;

(25) Appel has never fully reverse engineered a ROM chip from any voting machine;

(26) Appel is not aware of any computer programmers, outside of this litigation, who have developed a vote-stealing program that works in any version of the AVC;

(27) when the legitimate firmware is installed in the AVC, the votes get stored in four different ways: (1) added to the end of the audit trail file in the internal memory of the motherboard; (2) added to the candidate totals on the internal memory of the motherboard; (3) added to the audit trail file in the results cartridge; and (4) added to the candidate totals in the results cartridge. This record is kept up-to-date as votes are cast throughout the day of the election;

(28) if the internal memory on the voting machine fails, then the data is still there in the cartridge. If the cartridge fails, the data is still there in the internal memory and can be printed from both sources. Appel testified that this is a reasonable defense against inadvertent hardware failure;

(29) during the official election mode of his demonstration, after comparing all of the tapes, everything worked as expected on the voting machine;

(30) Appel testified that in his personal opinion, any acceptable rate of error for a voting machine should be well under one percent;

(31) there is no scientific literature that specifically says that an acceptable rate of error is less than one percent;

(32) the margin of error for the AVC is acceptable and well under one percent;

(33) the AVC compares well with other touch screen voting machines;

(34) the AVC gives adequate protection against over-voting;

(35) Appel did not conduct a study to measure interface error on the AVC;

(36) there are only two ways to install fraudulent firmware into the motherboard of the AVC, that is, through the ROM chip or the Z80 chip of each individual machine;

(37) Appel testified that if he were to design a vote-stealing program that would not arouse suspicion, he would limit the number of votes stolen on a given machine to twenty-percent;

(38) the fraudulent firmware will not cheat in the next election or in every election thereafter, unless the attacker only wants to steal votes from the candidate assigned to switch position H13 and the candidate he wants to receive the stolen votes is assigned to switch position E13;

(39) in one of the video-taped demonstrations, after Appel installed the fraudulent firmware, an audible error (a ringing noise) came from the voting machine;

(40) Appel agreed that a voting machine exhibiting an audible error would not be used in an election;

(41) Appel did not design a vote-stealing program that would manipulate votes based upon a candidate's name;

(42) if an attacker wanted to alter votes in a state-wide election, he would need to alter voting machines in more than one county;

(43) neither Appel nor anyone from his team of computer science experts ever designed a fraudulent vote-stealing Z80 processor chip;

(44) Appel does not know of anyone who has created a fraudulent Z80 processor chip that could go undetected in a voting machine;

(45) to remove the Z80 processor chip from the voting machine, the attacker must de-solder it, and then, re-solder the fraudulent Z80 chip. There is a risk of damaging the voting machine through the de-solder and re-solder process;

(46) malicious firmware on the daughterboard cannot steal votes from the motherboard;

(47) on the AVC Version 9, the daughterboard controls the audio function, which accommodates voters who wish to vote by audio; and

(48) the manipulation through the daughterboard will either cause the voting machine not to operate, or change the votes of those who vote by way of audio.

12. EDWIN BARKLEY SMITH, III (WITNESS FOR THE STATE)

A. BACKGROUND

Edwin Barkley Smith, III ("Smith") testified as an expert witness for defendants. In 1987, Smith graduated from Texas A&M University in College Station, Texas, with a Bachelor of Science degree in Mechanical Engineering Technology. In September 2003, Smith received a Master's degree in Business Administration from the University of Phoenix, concentrating in Management Information Systems.

From 1988 to December 2001, Smith worked for Ampex Corporation, Rockwell International, EFEH Associates, and K*TEC Electronics. Each of these positions required a background in manufacturing engineering. He has experience in programming ROM and EPROM-type devices, soldering of those devices, conducting circuit board and reliability tests, quality assurance and control management for a broad range of computers, environmental, electronics, medical, healthcare and telecommunication products, and federal governmental compliance in the environmental and telecommunication areas.

In December 2001, Smith joined Hart InterCivic, a manufacturer of electronic voting machines, as Operations Manager responsible for: (1) physical security of the computer infrastructure; (2) designing a protocol to prevent an intruder from infiltrating the computer network; and (3) hardware development for the security of the voting machines marketed and sold. During his tenure, there were no successful attacks.

Since May 2006, Smith has served as Vice President of Sequoia in charge of quality control and assurance, compliance, and certification. In this position, Smith interfaces with Federal and State regulatory agencies. Smith also provides updates to Sequoia regarding State legislative cycles, recently adopted legislation, voting system and technological changes, and manufacturing and logistical issues. Sequoia's Director of Quality Assurance reports to Smith.

Smith is a member of the American Society for Quality Assurance, and is certified in three professional areas as a: (1) quality manager; (2) quality engineer; and (3) quality auditor. Each certification requires extensive training and work related experience. Over the years, Smith has reviewed, researched and been responsible for handling a broad range of issues regarding physical security of computers. He has testified before various State Boards of Elections, Secretaries of State, the EAC and the House of Representatives Committee on Administration regarding voting system security.

Smith has authored approximately thirty publications, including a November 2008 article entitled, "Sequoia Voting Systems: Maintaining the Quality of the Vote." Additionally, Smith has been a guest lecturer at the Loyola School of Law and the John Marshall School of Law, both in Chicago. Lastly, Smith has participated in various panels pertaining to electronic voting systems.

Currently, the AVC and the Sequoia Edge are used in this State. The AVC is the most widely used machine in eighteen out of twenty-one counties. Over the years, Sequoia has sold 10,400 AVC machines to the State. While Smith was not involved in the 1987 recertification of the AVC, in November 2008, he examined many of the security features introduced by the State in the pending trial.

The court qualified Smith as an expert witness in the areas of certification procedures and compliance processes with respect to electronic voting machines, physical security of computers, quality control, and assurance methods of electronic devices. Smith, along with two others, co-authored Sequoia's response to Appel's report.

The sections that follow include information and recommendations offered by Smith during two days of testimony and from the joint report admitted into evidence.[59]

B. CERTIFICATION PROCESS

Smith testified extensively with respect to the certification and compliance process for electronic voting machines. The process begins with a technical documentation package ("TDP"), provided by the vendor that includes information regarding the development of the product, customer product information, troubleshooting manuals, operator manuals and maintenance manuals.

The TDP, the source code, and models of the hardware are delivered to a federal laboratory. At the federal laboratory, the ITA[60] engages in a multi-stage testing process. A laboratory must undergo an accreditation process originally prescribed by the National Association of State Election Directors ("NASED"), and currently established by the EAC. The last NASED certification was granted in October 2006. Once a laboratory is certified as an ITA, it then begins the multi-staged testing process involved with voting machines. The tests performed by an ITA are established by the federal Voting System Standards ("VSS"). Over time, two sets of standards and one set of guidelines have been established: (1) the 1990 version of the VSS, under which the AVC was certified;[61] (2) the 2002 version of the VSS, promulgated by the FEC;[62] and (3) the 2005 version, entitled the Voluntary Voting Systems Guidelines ("VVSG"), drafted and promulgated by the EAC. Voting systems that are certified to a specific standard are not required under the federal guidelines or federal law, to be recertified when a new standard is established. Instead, recertification to a newer standard is required only when mandated by state law.

Wyle, located in Huntsville, Alabama, is the ITA that performed tests on the AVC, both as to hardware and the firmware. Wyle performed an accuracy test on the AVC prescribed by the 1990 standards. To test accuracy, the 1990 standards use a test pattern or test script, whereby a person is given

---

[59] The two days of testimony are as follows: Tr. 1 (3/18/09) and Tr. 2 (3/19/09).

[60] Today, an ITA is known as a voting systems testing laboratory ("VSTL").

[61] According to Smith, the 1990 standards addressed accuracy and reliability.

[62] In 2002 there were enhancements to sections regarding accessibility, usability, hardware, and software.

a script directing them to vote for a specific individual. After the person votes, a second individual checks to make certain that the person did not make an error. The goal is to match the results of the mock election to the test script. According to Smith obtaining 287,000 ballots, without an error, means the machine has passed the accuracy requirement.

Based on Smith's review of the report issued by Wyle, the AVC also passed various reliability tests. The first part of the 1990 and 2002 standards test units dropped from various heights on multiple occasions to ascertain whether the unit handles shock. This emulates the type of handling that voting machines receive during warehouse preparation, as well as during transportation to the polling place and back to the warehouse. The second, a vibration test that is part of the 2002 standards, tests by placing a unit on a shaker table. This emulates the vibrations from the back of a truck, in order to determine whether the unit withstands transport. The third, a durability test, involves placing the unit in a humid chamber for forty-eight hours to evaluate the impact of temperature changes. Finally, other tests entail an increase and decrease in the normal wall outlet voltage to stress the equipment to points beyond the likely wattages at polling facilities.

According to Smith, an ITA does not certify voting machines. Instead, an ITA tests the product and issues a test report that may contain a recommendation as to certification. The process after an ITA tests the voting machines is the same under NASED and the EAC. Once an ITA tests the machine and the machine passes the tests, the test report is passed to either NASED or EAC, which are the certification bodies. If certified, the product is given a federal certification number. Obtaining a federal certification number permits the company to market the product in different states and work through state certification methods. According to Smith, the AVC received a NASED number. According to Smith, New Jersey's current certification procedures require a copy of the federal report from the ITA, as well as models of the hardware and software.

New Jersey uses WinEDS version 3.1074.[63] This version was federally certified in October 2006 and tested by Ciber Laboratories. According to Smith, Ciber is a federally accredited testing laboratory in good standing. According to Smith, WinEDS was subject to a certification process similar to that of the AVC, with the additional requirement that it undergo end-to-end testing. End-to-end testing involves a series of mock elections structured in a laboratory.

In response to a question from the court as to whether the hardware and software receive a separate recommendation from the ITA, Smith responded, "they can, but the place they come together is this end-to-end test because for the election management system to receive a test report, you have to have tested it with the voting machines." Tr. 1, 109:14-18. Smith also described various hardening processes in relation to WinEDS. Hardening involves altering settings within the operating system of the computer, in order to improve its inherent security, or taking steps to improve the inherent security of an object, such as computer networks.

While Smith did not know whether the software in the AVC had been modified since 1987, he testified that New Jersey requires recertification only if the new software impairs or changes the tabulation logic. When asked if alterations made in the software bear on the reliability and accuracy of the machines, Smith testified that the decision depends on the interpretation of a particular State's statutes and the requirements for certification and recertification.

The following questions and representations, regarding third-party vendor software used in the AVC and WinEDS, occurred during cross-examination:

> QUESTION: So then you can't possibly be aware of the testing performed on other third-party vendor software?
>
> ANSWER: No, that's not a true statement.
>
> QUESTION: Tell me how it's wrong.
>
> ANSWER: Regardless of whether it's one third-party vendor or a hundred third-party vendors, you're still going to package them together and compile them into firmware. That firmware then becomes part of the machine. The machine is then tested, as I testified earlier, for accuracy

[63] The WinEDS version is also referred to as 3.1.74 and 3.174 in the transcript.

> and reliability and a number of other things. I am familiar with those tests. So being that they are in the machine during those tests, those products are, in fact, tested.
>
> [Tr. 1, 179:14-180:1.]

C. REVERSE ENGINEERING

Smith testified there has never been any documented incident in which: (1) firmware of an AVC has ever been completely reverse engineered; (2) anyone has ever manufactured a fake AVC Z80 microprocessor containing fraudulent firmware; (3) a fake microprocessor was inserted into an AVC voting machine; or (4) a fraudulent ROM was ever placed in an AVC voting machine, other than in a pure academic setting, like the one created by Appel.

D. DESIGNING A FRAUDULENT Z80 MICROPROCESSOR

Smith challenged the conclusion by Appel that a FPGA can be used to counterfeit a Z80 prior to inserting the chip into the AVC. According to Smith, the silicon and the silicon etchings of a FPGA are immutable. As a result, it is impossible to etch a chip to look like a Z80 and then make it act like a FPGA, because they are non-forgeable. Smith characterized a fake Z80 chip with fraudulent software that works in the AVC as a fantasy and as pure science fiction. Tr. 2, 141:4-5. Finally, Smith testified that a FPGA used as a Z80 chip could be detected, in a laboratory setting, through the use of delidding, x-ray, or both, as explained below.

E. METHODS TO DETECT FRAUDULENT Z80

The Z80 is the microprocessor in the AVC. A microprocessor interprets firmware, the voter's output, the inputs of the poll worker through the operator panel, and executes what the firmware dictates. According to Smith, several detection techniques are available to determine whether a counterfeit Z80 chip with fraudulent firmware has been inserted into the AVC. These include delidding and x-raying.

At Rockwell International, Smith performed delidding in the material evaluation laboratory to examine silicon wafers in devices that had failed or were suspect for some reason. Delidding is defined as an examination of electronic devices, and involves removing the material on an electronic component, such as the covering over the working part of the chip.

Smith explained delidding as a process in which nitric acid is dropped onto the center of the Z80 chip. After a few hours, the nitric acid dissolves the black plastic covering that permits an individual to examine the gold microscopic wires in the chip with the naked eye, a standard visual microscope, an electron microscope or x-ray. Though described by Smith as a destructive testing process, in which the chip becomes unusable and the voting machine requires a new chip, he testified that delidding would successfully detect whether the Z80 chip is real or not. Smith has used hardening techniques, such as delidding, to examine and improve the physical security of machines and computer systems.

During cross-examination, Smith acknowledged that no state has used delidding to test voting machines for fraudulent software. The cost of delidding is in single dollars per unit when done in volume. While it takes a good deal of skill to desolder a voting machine, Smith testified that it is not difficult to master the skill. However, delidding requires that the circuit board or chip be sent off-site from a voting warehouse.

X-raying is another method that may be used to discover whether a fraudulent Z80 has been inserted into an AVC. Unlike delidding, it is a non-destructive testing process. The process involves using an x-ray machine to tightly focus on a particular area of a chip, in order to view fine features inside the chip at varying depths. To use an x-ray to detect a fraudulent Z80, the entire circuit board must be removed and sent to an outside entity. Smith did not know whether any outside entities perform this service in New Jersey.

Smith, when employed by K*Tec Electronics, used x-ray methods as part of his quality assurance duties for examination of electronic devices. The process is commonly used to examine circuit boards to test the integrity of the component. The x-ray machines produce a high resolution, comparable to medical imaging equipment. To obtain the type of quality demonstrated by the photographs shown in the report, a $300,000 machine is most likely required. Smith testified that this type of equipment will detect a fake Z80. When Smith was shown photographs, the following exchange occurred:

> QUESTION: Do those photographs accurately reflect the physical state of a comparison between a legitimate Z80 chip and a fraudulent FPGA?

> WITNESS: Yes, they do . . . as I mentioned earlier, the silica etchings are so very different between a real and a counterfeit Z80.
>
> [Tr. 1, 153:23-154:1-8.]

Another technique is to measure electromagnetic radiation or radio waves. A fraudulent Z80 chip would not radiate the same radio signals as a true Z80. The device used to measure and determine an electromagnetic signature is akin to a television antenna. This testing takes only a few minutes on each voting machine. Smith described this technique as completely non-destructive, not intrusive to the machine and able to provide information right away if something has been electronically tampered with inside the machine. During questioning, Smith was asked by counsel for the State:

> QUESTION: Based upon your training and experience would that technique of radiating electromagnetic energy detect a counterfeit Z80?
>
> ANSWER: Yes, it would.
>
> [Tr. 1, 167:14-17.]

On cross-examination, Smith testified that to his knowledge no state has used delidding, x-raying or electromagnetic radiation to test for a fake Z80.

At the end of direct examination, the State asked a series of questions about the AVC:

> QUESTION: Mr. Smith, have you ever learned that an election result was wrong because of the AVC Advantage machine?
> ANSWER: In terms of candidate tallies, who won, who lost, by how much, no.
>
> QUESTION: Have you ever learned outside the academic setting that an AVC Advantage Version 9 was ever hacked?
>
> ANSWER: No.
>
> [Tr. 1, 168:11-19.]

F. DAUGHTERBOARD

Smith challenged the notion that fraudulent firmware could be installed on the daughterboard through an audio ballot cartridge corrupted with fraudulent firmware. He testified that it is not possible.

G. HARDENING METHODS, ANTI-VIRUS SOFTWARE AND HEURISTIC CHECKING

According to Smith, EAC guidelines for election management and Sequoia both recommend hardening and anti-virus software for election management systems such as WinEDS. There are methods for hardening the computers on which WinEDS operates to prevent viral infection, as previously noted. Hardening involves taking steps to improve the inherent security of something; in this case, computer networks. In response to questions as to whether there exists any ways of strengthening or hardening the computers to prevent virus infiltration into the WinEDS computers, Smith stated:

> [y]es, there is. There are in the hardening guidelines there are over a hundred different steps, each of which plug some vulnerability present in Windows or raises the hurdle significantly higher to intrusive software of any sort. Some even help out with potentially malicious people that would want to get on the system undected and undeterred and render attack upon the system.
> [Tr.1, 117:17-24.]

On cross-examination the next day, Smith noted:

> There are 105 steps, but most of them are automated, meaning that we provide a package. It's a small piece of software that essentially goes in and does 90 plus of those steps. I forget the exact number. The remaining few you have to do by hand.
>
> [Tr. 2, 88:16-20.]

As to the time required to run the script, he testified "it takes less than about a minute to run." Tr. 2, 89:11-12.

As noted heretofore, each step is designed to plug up vulnerabilities present in Windows or to raise the hurdle in order to bar intrusive software or malicious persons. About ninety percent of these steps can be completed by executing one piece of software, provided by Sequoia for free. It takes less than a minute to do this and once executed, the hardening process is almost complete. The hardening steps only have to be done once for each machine and not for every election.

Another hardening method is to never connect WinEDS enabled computers to the Internet. Sequoia recommends that election related computers never be connected to the Internet, but instead be maintained on an isolated network. The EAC also recommends this in the election management guidelines. Still another method involves reloading WinEDS before each election.

Smith supports anti-virus software and heuristic checking. Heuristic checking is technology that is often included in the leading anti-virus programs. While anti-virus programs search for viruses matching the prescribed viral definitions, heuristic checking looks for codes that resemble viruses or exhibit computer viral-type behavior. Both of these are hardening methods as well.

Smith also discussed physical access controls and logical access controls. Physical access controls regulate access to election central computers, thereby barring any type of malicious attack. The controls may be comprised of any or all of the following: (1) card keys, badges, surveillance cameras, locks, and keys on doors; (2) the placement of the computer room in a certain building; (3) different layers of fences around the building; (4) guards; and (5) alarm systems.

In terms of logical access controls, WinEDS 3.1074 provides the opportunity to assign users and roles. Users are the various names and passwords of individuals given access to the WinEDS system. An individual may be permitted to access the entire system, or be permitted to access less information, such as the database or election definition. Roles involve locking individuals out of certain areas, but permitting access in other areas in order to allow successful completion of job functions.

If all of the techniques detailed by Smith fail, it is possible to wipe out the central computer and reload the Windows operating system, WinEDS, or both. Different states routinely reload the machines at various times in the election process. States may receive a clean copy of WinEDS from federally accredited laboratories that maintain a copy of the software, after the testing process is finished. The laboratories maintain copies of this software in a safe. After obtaining a copy of the software, states remove the WinEDS on their existing machines and make copies for every county. The cost, borne by the vendor, includes purchasing a CD, Federal Express charges, and approximately thirty minutes of laboratory time.

In response to the time involved, the following dialogue occurred:

> QUESTION: How much time is involved for, say, a medium-sized county to wipe out their WinEDS computers and then reinstall a clean copy of the WinEDS program?
>
> ANSWER: Time, medium size county. To reinstall.

> COURT: Well, if he has any personal knowledge. How long does it take to reinstall WinEDS on a machine?
>
> WITNESS: I have seen it done in four hours for a medium-size county, several hundred thousand registered voters.
>
> COURT: How many machines?
>
> WITNESS: These particular counties will generally have one server. They may have a primary and redundant server, and then they'll have anywhere from one to a half dozen laptops that they also have WinEDS on in order to aid them in writing before election –
>
> COURT: How many methods do they have for installing it on the machine and how many machines do they have?
>
> WITNESS: To some extent, your Honor, they can do them at the same time. If they receive a copy of the CD from the State, they can make their own copies, they can put one in every machine and it will take roughly four hours and they'll be done. They don't have to attend to the process the entire time, which is nice. It takes about four hours.
>
> QUESTION: Based upon your training and experience and your knowledge of hardening computers, if a county uses one or more of these methods, do you have an opinion of whether this would prevent the virus infiltration of the WinEDS computers?
>
> ANSWER: Yes, I believe that if the hardening is properly and fully applied it would prevent the virus's infiltration along the lines of that espoused by Dr. Appel's report.
>
> [Tr. 2, 126:5-127:19.]

While the hardening guidelines are available to clients, Sequoia does not monitor the implementation of those guidelines. The hardening guidelines contain over one hundred steps, but most are automated and provided in Sequoia's software package.

The software executes approximately ninety steps and the rest must be completed manually. According to Smith, it does not take a great deal of expertise in enterprise network security management to understand Sequoia's hardening guidelines. Therefore, a reasonably skilled IT person may readily understand the guidelines. Sequoia's software package runs in approximately one minute. The software is provided when Sequoia is doing installations, and if someone from New Jersey contacts Sequoia and requests the software. If so, the software is provided free of charge.

Smith does not know whether New Jersey has implemented the hardening guidelines on a county-by-county basis. While it does not appear the hardening guidelines were implemented in Union county in connection with the February 2008 election, the guidelines would not have disclosed the option switch anomaly, nor recognized a virus. The goal of hardening is to prevent infections in the first place and block any vulnerability in Windows.

Smith also emphasized the need to distinguish between hardening guidelines and an anti-virus program. Since WinEDS does not have an Internet anti-virus program, Sequoia recommends that jurisdictions select an anti-virus program, or select one Sequoia recommends from a list of vendors. Smith believes an anti-virus program is important to the integrity of the product.

Smith testified that anti-virus programs do not cover all possible viruses and that updates are normally distributed through the Internet. Although Smith does not recommend connecting election computers to the Internet, it is possible to use a CD or USB stick to install these updates on WinEDS computers. Also, astute jurisdictions put updates on one computer, not attached to the elections network, in order to prevent any potential mishaps. Then, the CD or USB stick is placed into all the election computers in order to update them. Smith is aware of jurisdictions that practice this method outside of New Jersey.

Smith recommends both hardening and anti-virus software, which is consistent with EAC guidelines for election management, but not for individual machines. Instead, these methods relate to remote stations for transmission of votes and the servers in the election warehouse or Clerk's office. On cross-examination, the court asked the following:

> COURT: When you're talking about hardening and anti-virus software, you're not talking about on the individual machines. You're talking about on the machine, like when they're taken to the Municipal Clerk and they're transmitted electronically in some way to the County Clerk for the transmittal of votes, that's what you're talking about, the hardening and antivirus?
>
> WITNESS: Yes, ma'am. I'm talking about any remote stations for transmission of votes, and I'm talking about the servers that are downtown in the elections warehouse or the County Clerk's office,

> wherever they reside, those machines, this is for protection of those machines.
>
> COURT: And so the only security measure that you're talking about for the voting machine would be the physical things that we talked about, like locks and keys and those kinds of things?
>
> WITNESS: Yes, ma'am. The security of the voting machine relies on two items, two classes of items: one, the physical security, and two, the inherent security from the architecture of the hardware and software in the machine.
>
> [Tr. 2, 109:2-24.]

Smith testified that, in terms of safety, to avoid the possibility of a virus infection to the Microsoft Windows operating system, as well as or separately from infecting the WinEDS operating system, some jurisdictions clean out and reinstall Windows and WinEDS.

Regarding machines with a VVPAT, Sequoia recommends hardening and anti-virus software also, inasmuch as the EAC still requires a certain level of protection despite software independence. Smith claims that it is impossible to impact a machine with a VVPAT and skew the results because a reasonably attentive voter would notice. In New Jersey, voters get three chances to vote, so a voter may go back and try again if the machine is voting wrong. If the machine votes incorrectly a second time, a voter most likely would leave the booth and inform an attendant of the problem.

H. FIRMWARE VALIDATION

Smith reviewed two methods of firmware validation to detect a fraudulent ROM: hashing and bit-by-bit comparison. As to the bit-by-bit comparison, he noted:

> [t]here are machines that are available from third party vendors - - nothing to do with Sequoia. Sequoia has no business interest in these companies - - that you can – they have sockets that you can insert ROM chips, you can insert other varieties of chips in there, any chip containing software, and you can put a known good chip in there, once again, that you can get from the federally accredited laboratories or a known good source, and then you can take - - and next to it in a different socket you would put the ROM chip under test. You push the button on the machine and the machine does a bit-by-bit comparison, bit-for-bit meaning every nook and cranny, nothing can hide inside those ROM chips and it goes through the entire ROM chip and if there's any difference between the two, it reports those differences back to you.

[Tr. 1, 140:7-25.]

This process takes under two minutes on one machine, not including the time needed to establish the test. The machines are relatively inexpensive depending on the size and the number of sockets. As an example, this technique is used in California, Nevada, in Cook County, Illinois, and the City of Chicago. It can be used for pre-election testing, post-election testing, or both. Instead of testing all of the machines, a sampling plan can be developed in accordance with the American National Standards Institute or United States military.

With respect to the hashing method, a hash is a fingerprint on a piece of software. Hash functions are mathematical functions approved by the federal government. Information on ROM chip firmware is run through hashing algorithms, which produce a stream of numbers and letters representing a fingerprint of that software. As Smith testified:

> You can take your body of software, in this case we take what's on a ROM chip firmware and we would run it through that hashing algorithm, and out of the hashing algorithm would come a stream of numbers and letters which represents a fingerprint, to use a colloquial term, of that software and any change to that software, even one bit, will change the hashing value that you would get if you ran that code through that hashing function. And the changes of two files hashing to the same hash value at the end is something like one in over 4 billion so you're pretty safe to have that hash number one in 4 billion.
>
> So then you can take any from the federal labs because they're required by the government to hash all the software that they approved. You, the jurisdiction, can obtain the hash values regarding a particular piece of software or firmware. As I mentioned earlier, you can do that through WinEDS as well as firmware.
>
> And then you can utilize these machines - - you can place the ROM chip that you're testing into the machine, and instead of having to do a bit-for-bit comparison, you can have it bring up the hash value of that software. You then have the known good hash value from the federal lab, you look at it, you look at the machine display; and if they are the same, then you can be assured that the software inside that ROM chip is the same as what the federal lab tested.
>
> [Tr. 1, 144:22-145:24.]

Any alteration in the software affects the hashing value as a result of running the code through the algorithm. A jurisdiction may obtain known good hash values for a particular piece of software or

firmware from a federal laboratory. The validity of a ROM chip may be determined by comparing the known good hash value with a hash value obtained by a particular ROM chip. This test requires two minutes, not including loading and unloading time. Smith testified that if election officials employed the hashing method, they would be able to detect fraudulent insertion of firmware into a ROM chip.

Smith testified that there is a method of validating software, either before or after the election, to determine whether there has been any fraudulent software or firmware used in the voting machine. Smith references third-party hashing programs. It is possible to take the third-party piece of software that is hashing the algorithm, and hash the WinEDS installation on the computer, or the main WinEDS program with the tabulation logic. Federal labs have the hash value for WinEDS on file and can provide it to jurisdictions using some reasonably secure method. Additionally, there is third-party software available to compare the hash value of WinEDS with the value received by the federal laboratory. If the values are identical, then the WinEDS program has not been tampered with.

Smith testified that the bit-by-bit method of firmware validation is successful in detecting the insertion of fraudulent firmware into ROM in voting machines. In terms of testing methods, Smith feels the bit-by-bit comparison is the best method to assess the integrity of ROMs on the machines, because it is a direct comparison of every nook and cranny inside the ROMs. However, Smith believes that hashing is more definitive for assessing the integrity of WinEDS because it is a software program that is on a hard disk inside a computer. In Smith's opinion, hashing results in essentially 100% reliability.

Nevada, using the Sequoia Edge 2, performs pre-election and post-election firmware checks. A hash method is used to check the chips. ROMs must be removed from the motherboard, requiring the removal of each security seal affixed to the board. After performing the tests, the ROMs and fresh copies of the security seals are reinstalled. In response to questions by the court, Smith testified:

> [y]es, ma'am. The State of Nevada, we have a state-wide contract. They use the Sequoia Edge 2, which is similar to the DRE used in Salem County, New Jersey. And yes, your Honor, they perform pre-election and post-election firmware checks. I'm not sure if it's 100 percent of the machines, or a sampling of the machines, but I know from my conversations with them that when they did that the first time, they did

do 100 percent of the machines, but they came out of it from a known, good starting point, and then they went forward.

COURT: So the firmware check would be the hash?

WITNESS: Yes. In this case, they used a hash method.

COURT: And do they check the ROM chips?

WITNESS: That is what they're checking, They're pulling out the firmware containing chips. In those machines, it's not a ROM, but that's really neither here nor there for this discussion.

COURT: You said that bit-by-bit was better for chips.

WITNESS: For ROM chips it is, yes.

COURT: How about these chips?

WITNESS: These chips are of a different type. They are exactly a compact flash card, so the hashing method is better. Although you can do bit-by-bit on them as well.

COURT: And they do it pre and post election?

WITNESS: Yes, ma'am, they do.

[Tr. 2, 119:12-120:21.]

Interestingly, Smith testified that Sequoia recommends hardening and anti-virus software for DREs with VVPATs in order to provide protection to Election Central. Once again, in response to questions from the court, Smith noted:

COURT: Is it your testimony that the hardening and antivirus software is still recommended for the machine with the VVPAT?

WITNESS: Yes, ma'am, it is.

COURT: Okay, and why is that?

WITNESS: Well, because you still - - there's no reason to allow your Election Central computers to be at any greater risk to infection from a virus or what not than you would have under any other circumstances regardless of the technology in the polling place. Whether that's optical scan, hand-counted paper ballots, DRE, with or without VVPAT is not material.

[Tr. 2, 124:2-14.]

I. ANOMALIES OR BUGS

Smith explained the option switch bug and tilde issue. The option switch bug resulted from misuse of the operator panel by the poll worker. Regarding the February 2008 primary election, Smith personally recreated the option switch bug in order to design a remedial prototype. The prototype, distributed across the State, is comprised of a clear plastic cover with two pieces of Velcro. Smith manufactured aluminum templates that fit into a recessed area of the AVC operator panel. The aluminum templates provide the location of the two pieces of Velcro that attach to the operator panel. Upon removing the aluminum templates, the Velcro remains and lines up with the plastic cover designed by Smith. In the June 28, 2008 primary, Smith did not receive any complaints regarding the option switch bug.

Smith testified that the option switch has been fixed in the D-10 by changing the firmware code to initialize a variable that was not initialized in Version 9.00H. During cross-examination, regarding whether the option switch issue rendered the AVC unreliable, the following testimony was elicited:

> QUESTION: So the fact that it generated inaccuracies doesn't mean it's unreliable to you?
>
> ANSWER: No. It means that the party turnout totals when the button is - - when the operator panel is misused by the poll worker and errant buttons are pressed it does provide an inaccurate total.
>
> QUESTION: Certainly that's an accuracy issue, isn't it?
>
> ANSWER: No, because accuracy is your candidate totals, your candidate tallies, over- votes, under-votes. So in terms of, once again, declaring who won, who lost and by how much, no, because that was not affected. So, thus, it is an undesirable situation, it shouldn't happen and needs to be fixed and it is fixed. Is the machine inaccurate? No.
>
> [Tr. 1, 187:9-24.]

The tilde problem involved a candidate by the name of Carlos Cedeno. Since WinEDS had not been programmed to include the tilde, his name did not appear with a tilde symbol above the "N," and his name did not appear on the summary report. If properly programmed, this would not occur.

Smith described another issue where the candidate's name did not appear on the summary report. The candidate was assigned a numerical candidate ID of 999. There is a bug in WinEDS 3.174, causing candidates with an ID of 999 to not appear on the summary report. There are approximately twenty reports printed by the AVC. The only one where ID 999 was omitted was the summary report. As a result of the issue in Union County, Sequoia issued a product bulletin. Regarding this issue, Smith responded to questions from counsel and the court:

> QUESTION: Is there a way to reassign a candidate if the system assigned a candidate to the slot 999?
>
> ANSWER: Yes, you can view - - through WinEDS you can view the database and see if the candidate does have the 999 candidate ID in the database in a human viewable form. . . .
>
> COURT: How often would you see that 999?
>
> WITNESS: Only once, and only if you had a thousand candidates in a particular election.
>
> COURT: That's the only time you would see that, a thousand candidates in a particular election district or –
>
> WITNESS: No, since election databases are done via the county, it would be that county.
>
> COURT: So you need more than a thousand candidates on the ballot for that 999 ID to show up?
>
> WITNESS: Across the county.
>
> COURT: Across the county?
>
> WITNESS: Yes, ma'am
>
> COURT: In your experience does that happen very often?
>
> WITNESS: No, it does not happen very often, but it does happen.
>
> COURT: Okay.
>
> QUESTION: The issue with the 999, does that in any way affect the vote totals for the candidate?
>
> WITNESS: No, it does not.
>
> [Tr. 1, 135:8-136:19.]

Smith described a buffer overrun in the software code as a situation in which software has a finite capacity of data. If an attacker attempts to put more data into that area, thereby exceeding the capacity of the buffer, this may cause secondary effects resulting in a shut-down of the machine. This impacts voting by necessitating a restart of the machine. After the machine recovers, the public counter is used to determine whether the vote was counted or not. At most, this would cause a ten-minute delay. Smith concedes that this bug may shut down the machine repeatedly, requiring the use of a new machine or emergency ballots.

J. USER INTERFACE ISSUES

Smith testified that the AVC alerts voters that they have not voted for certain offices. Further, the chirping sound the AVC makes is measured at 66 decibels, whereas normal conversation is measured at around 40 decibels. Smith challenged the notion that the user interface is inadequate.

K. PREVIOUS VERSIONS OF THE AVC

According to Smith, none of the upgrades to the AVC, from its previous versions since 1987, have changed the vote counting logic associated with the machine. Furthermore, outside the controlled environment created by the court ordered examination, Smith has never heard of an erroneous election result on the AVC. Nor has any evidence been produced to establish that fraudulent firmware has been introduced.

During cross-examination, Smith acknowledged that: (1) the option switch bug caused problems in eight New Jersey counties and slipped through Sequoia's quality controls and any external examination process, including ITAs; (2) the option switch bug was not detected in Pre-LAT; (3) the option switch bug was not detected in the certification process; (4) the net effect of the option switch bug as manifested in the February 2008 election was that the AVC was activated with the wrong primary election ballot for many voters; (5) anyone could remove the plastic cover, affixed with Velcro, although it is likely that they may break it; (6) it would be difficult to accidentally take off or knock off the plastic cover because it

fits into a partial recess in the operator panel; and (7) he is unsure whether there is a system in place to monitor whether someone removes the Velcro or plastic cover, because that is a jurisdictional issue.

L. SOFTWARE INDEPENDENCE

Smith defines software independence as the ability to recount and check the results of an election, independent of the software running on the machine used. Through a record of cast votes, it is possible to count the election results and be assured that the tabulation is accurate, regardless of unknown software bugs, malicious alterations to software, or inadvertent changes. According to Smith, a VVPAT constitutes a software independent mechanism. He noted that Sequoia possessed the technology to develop a VVPAT in 2003, and deployed this technology in 2004, two years before the statute passed in New Jersey. Smith believes that Sequoia is the sole vendor providing a cut-and-drop system in the United States. Sequoia first produced a computer system, available for purchase, using the cut-and-drop method in late 2006. This feature is part of the AVC D-10.

M. CONNECTION TO THE INTERNET

Sequoia recommends to customers that election computers remain disconnected from the Internet. EAC includes the same recommendation in its election management guidelines.

N. STORING AND DELIVERY OF MACHINES

Sequoia recommends standards regarding storage such as temperature and humidity, required by the federal government as part of the technical documentation package. While the modes of delivery vary across the country, Sequoia does not recommend to customers that voting machines leave the election warehouse sealed and locked.

O. REPORT BY APPEL CHALLENGED IN JOINT REPORT

In their joint report, Smith and Paul David Terwilliger ("Terwilliger") challenge many of the conclusions made by Appel. For convenience, these are listed below:

> (1) vote data is written to the results cartridge after each voter, and at all times the internal memory and the results cartridge storage must be identical or the machine will halt;

[Report, § 2.5, p. 3.]

(2) the term “correct in all circumstances” is an impossible standard;

[Report, § 2.7, p. 4.]

(3) security screws installed with security caps deter removal and prevent undetected tampering;

[Report, Figure 1, p. 5.]

(4) the plastic strap seals cannot be easily defeated. The strap is only intended to evidence unauthorized removal;

[Report, § 5.7, p. 6.]

(5) if the seals can be substituted because the serial numbers are not routinely logged, this is not a failure of the AVC, but a State and County procedural issue that is equally valid for every voting system that has ever been created;

[Report, § 10.6, p. 7.]

(6) New Jersey has made sure that custom printed serialized tamper-evident seals are available through the State, and has provided instructions for their use in all counties;

[Ibid.]

(7) without a method for successfully re-installing the reverse engineered firmware, this reverse engineering exercise is a waste of time;

[Report, § 11, p. 8.]

(8) new voting machine software is typically introduced to the marketplace every year or two. New voting machine firmware would lay waste to any ongoing reverse engineering program;

[Ibid.]

(9) all of the fanfare around reverse engineering is at best misleading since the academics offer no method to actually put reverse engineered firmware into a voting machine or to keep up with new firmware introductions from Sequoia;

[Ibid.]

(10) fraudulent replacement of the microprocessor is either deterred or detected by the seals. Also, it does not pass the common sense test that an army of hackers could visit all or most of the over 10,000 machines,

carry un-noticed the bulky de-soldering tool, de-solder, remove and replace the microprocessors, make sure the now-faked AVC actually works, and then put all of the sheet metal and security devices back in place without providing evidence of their crime and without damaging the AVC;

[Report, § 12, p. 9.]

(11) a fake AVC process does not exist. Frankly, the entire notion is a fantasy;

[Report, § 12.14, p. 9.]

(12) third-party software is commercially available to perform pre-election and post-election firmware validation;

[Report, § 14, p. 10.]

(13) the use of VVPAT meets the EAC's definition of software independence. The model AVC recently, successfully tested by the New Jersey Institute of Technology and currently under consideration for New Jersey State Certification contains a VVPAT;

[Report, § 16, p. 10.]

(14) the virus described by Appel can only lead to a denial of service attack on the AVC audio subsystem. Such a virus cannot "infect" the main systems of the AVC through the audio board. An infected audio cartridge would not be inserted in this set of voting machines;

[Report, § 21- 23, p. 11.]

(15) safeguards currently in use would stop any viral infestation and, in fact, eliminate it from the WinEDS computers. This includes the practice of reloading WinEDS from a clean copy just before each election cycle, so that if a virus did infect a WinEDS computer, it would be removed, and any malicious software likewise removed when the computer was reloaded with the fresh copy of Windows and WinEDS. This process requires less than four hours per election cycle in a medium sized county;

[Report, § 21-23, p. 11-12.]

(16) the so called "barely audible chirping sound" is actually emitted by the AVC at a sound level well above the level of conversational speech. Also, the booth light is not fluorescent;

[Report, § 29.3, p. 12.]

(17) some percentage of voters do not complete the act of casting their ballot, but this is not due to DRE technology or the user interface of the AVC;

[Report, § 30, p. 13.]

(18) the claim that the user interface of the AVC provides for a high level of under-votes or skipped contests by the voter is not supported. The available option to light all contests that the voter may vote on should be enabled for an optimum user interface. Union County used the worst possible configuration option, that of NOT lighting the contest names until they are fully voted;

[Report, § 33.1, p. 14.]

(19) while one can see the voter's hand moving when it is close to the ballot face on the machine, it is not possible to see the voter's finger actually press the selection button nor determine how the voter voted; and

[Report, § 35, p. 14.]; and

(20) the academics omit the fact that the AVC 9.00H has been certified only to the 1990 FEC standards, not the 2002 VSS.

[Report, § 36, p. 15.]

P. POINTS RAISED BY PLAINTIFFS ON CROSS-EXAMINATION

During cross-examination, Smith acknowledged:

(1) fraudulent firmware can be installed in an AVC voting machine;

(2) fraudulent firmware can be written to maintain the count of the AVC public counting;

(3) it is theoretically possible for fraudulent firmware to be designed so that it won't misallocate too many votes, thereby avoiding detection, although it is extremely difficult;

(4) it is theoretically possible to design fraudulent firmware so that it will not be caught in pre-election logic and accuracy tests, although the hurdles are extremely high and a slight mistake makes fraud detectable;

(5) the lock on the back of the AVC can be picked, although it is not easy and it does not provide unfettered access to the results cartridge, computer chips, and circuit board;

(6) it is theoretically possible that fraudulent firmware or a virus could be so well written that it could overcome diagnostic tests;

(7) an individual may purchase a Sequoia voting machine off the Internet, although Sequoia tracks such machines as such sales indicate violations of licensing agreements with counties because Sequoia has the

right of refusal; and

(8) if it could be done, an FPGA programmed to simulate the Z80 chip would raise a concern, although Smith is not aware of this ever being done.

Q. POINTS RAISED BY STATE ON RE-DIRECT EXAMINATION

Counsel for the State reiterated the following points:

(1) the sound level of the AVC measured 66 decibels; normal conversation is around 40 decibels;

(2) Version 9 can deselect a write-in vote;

(3) there has never been a documented incident where the firmware of a Version 9 was ever successfully totally reverse engineered;

(4) there has never been a documented incident where anyone has ever manufactured a fake AVC Z80 microprocessor containing fraudulent firmware;

(5) there are no known incidents where a fake microprocessor was ever inserted into an AVC voting machine; and

(6) there are no known incidents where a fraudulent ROM was ever inserted in an AVC, other than in an academic setting.

R. CONCLUSION

Sequoia recommends in its promotional literature and customer manuals for governmental agencies to implement hardening guidelines. According to Smith, if implemented, all of the alleged security vulnerabilities and inaccuracies alleged by Appel can be remediated. Also, Smith testified there is evidence of vote-stealing with paper based voting systems, which include punch card systems, optical scanner and hand-counted paper ballot systems and lever voting systems.

13. PROFESSOR MICHAEL IAN SHAMOS (WITNESS FOR THE STATE)

A. BACKGROUND

Shamos graduated from Princeton University with a Bachelor of Science degree in Physics in 1968 and a Master of Science degree in Physics from Vassar College in 1970. After graduating from Princeton, while studying at Vassar, Shamos worked full-time for the IBM Corporation as a computer programmer. From 1970 to 1972, he worked for the National Institute of Public Health Service ("NIH")

in Bethesda, Maryland, as a supervisory programmer at the National Cancer Institute. While at NIH, Shamos attended American University in Washington, D.C., and earned a degree in Technology Management. Technology Management "has to do with analytical techniques in optimizing and improving manufacturing processes."[64] Tr. 1, 10:23-25.

By 1972, Yale had started a Computer Science program. Shamos applied for and was granted admission in 1972, and started that year. Though he left Yale after three years to accept a position at Carnegie Mellon University as an assistant professor, he completed his Ph.D thesis in absentia and received a Ph.D. from Yale in 1978 while a full-time faculty member. While at Yale, he was admitted as a fellow to Sigma Xi, a science honorary society, and was the recipient of the IBM Fellowship.

Shamos is a long-time member of the Society for Industrial and Applied Mathematics ("SIAM"), and was named SIAM national lecturer in 1977 and in 1978. He also received temporary appointments to the University of Rochester and McGill University as a distinguished lecturer in computer science.

In 1981, Shamos graduated from Duquesne Law School and was admitted to both the Pennsylvania bar and patent bar the same year. While at Duquesne, he was elected to Law Review. After law school, he practiced in the Pittsburgh area, specializing in intellectual property and computer law. Affiliated with Carnegie Mellon University for thirty-four years, Shamos holds the title of Distinguished Career Professor in the School of Computer Science. The founder and Co-Director of the Institute for eCommerce at Carnegie Mellon, since 1999 he has taught courses in eCommerce Technology, Electronic Payment Systems, Electronic Voting, and eCommerce Law and Regulation. One course, entitled "Electronic Voting Systems," covers electronic voting systems, federal and state regulations, and a broad range of issues related to the administration of elections.

Currently, Shamos directs a graduate degree program in eBusiness Technologies. He has also taught in the Department of Mathematics, Statistics, the School of Business, and the Heinz School of Public and International Affairs. In addition, he has an academic appointment at the University of Hong

[64] The three days of trial testimony are referred to as follows: Tr.1 (3/23/09); Tr. 2 (3/24/09); and Tr. 3 (3/25/09).

Kong in the Department of Computer Science. In 2004, he developed a course entitled, "Electronic Voting Systems," which focuses on electronic voting systems and administrative procedures that relate to how elections are conducted and the various participants in the process.

From 1980 to 2000, Shamos served as one of three members of the Voting Machine Committee for the Commonwealth of Pennsylvania. During that period, he participated in every electronic voting system certification examination. In 2004, after HAVA, 42 U.S.C. 15301 et seq., the State disbanded the panel of three examiners and replaced it with one consultant, designated by the Secretary of the Commonwealth ("Secretary"). Today, Shamos is one of the two consultants appointed by the Secretary.

In 1986, at the request of the State of Texas, Shamos testified before the Legislature. One year later, and continuing until 2000, he served as a voting machine examiner for the State of Texas. During that period, he participated in every electronic voting system certification examination.

In 2006, Shamos was hired as a consultant for NIST, now part of the Department of Commerce, to teach a course to internal staff on how to test voting equipment.[65] The same year, he was hired by the State of Massachusetts to conduct a security review of their electronic voting systems. He was also hired by the State of Florida, regarding an election in Congressional District 13, as a member of the Sarasota Source Code Audit Task Force. Shamos has served as a member of Project SERVE, a project funded by the military to oversee the Department of Defense plan to provide servicemen the opportunity to vote over the Internet. When the States of Nevada and Delaware adopted electronic voting machines, Shamos was hired as a consultant.

Nationally recognized as an expert in electronic voting systems, he has testified before numerous federal and state legislative and administrative bodies regarding electronic voting systems. This includes: (1) the Texas Legislature; (2) the Pennsylvania Legislature; (3) the United States Commission on Civil Rights; (4) the U.S. House of Representatives; (5) the Committee on House Administration; (6) the Virginia Legislature; (7) the EAC Technical Guidelines Development Committee; (8) the House Ways and Means Committee of the Maryland General Assembly; and (9) the Georgia State Board of Elections.

[65] NIST has a statutory role under HAVA to advise the EAC on guidelines for testing voting systems.

He has testified in approximately six reported cases in both the state and federal courts. Over the years, he has examined for certification 121 voting systems, of which at least half have been DREs.[66]

The author of several articles on computers and computer security, Shamos has served as Editor-in-Chief of the Journal of Privacy Technology and is on the editorial boards of Electronic Commerce Research and the Pittsburgh Journal of Technology. Since 1980, he has conducted research or studies in the field of electronic voting systems and electronic voting systems certification. Many of the articles have been printed in peer reviewed scientific journals. He has also written papers for NIST and was commissioned by it to prepare a glossary of electronic voting terms and procedures. In addition, he has attended and lectured at prestigious conferences throughout the country for organizations such as the Association for Computing Machinery, and the National Academy of Engineering,

Shamos has qualified as an expert witness for plaintiffs and defendants in the field of computer science, electronic voting systems, electronic voting system certification, election administration, electronic voting system security, electronic voting system regulations, standards, guidelines and the history of voting. Accepted by the court as an expert, Shamos was permitted to testify as to each of the aforementioned areas.

During his deposition, Shamos was asked whether he had an opinion as to the accuracy and reliability of the AVC. He responded that he was not hired to render that opinion. Rather, he was hired to respond to the Appel report. At trial, plaintiffs raised this issue and objected to Shamos testifying as to the accuracy and reliability of the AVC. The State did not object. While Shamos did not offer an independent opinion as to the accuracy or reliability of the AVC, he commented on the conclusions reached by Appel. As noted on cross-examination:

> QUESTION: And you've testified repeatedly that you offer no expert opinion as to the security or accuracy of the AVC Advantage 9.00H; is that correct?

[66] To prepare for an examination in Pennsylvania, he reviews all of the documentation before traveling to Harrisburg to conduct the examination. The typical examination lasts approximately nine hours. Each examination is open to the public and is recorded. After reviewing all of the materials, he then prepares a recommendation to the Secretary.

> ANSWER: No. What I've testified is that I will not be offering an independent opinion on the accuracy or reliability, but I certainly have commented at great length on Dr. Appel's opinions on accuracy and reliability.
>
> [Tr. 2, 104:18-25.]

Shortly thereafter, Shamos explained, "if you asked me, are the machines used in New Jersey accurate, I will not offer an opinion on that. If you ask me, are they reliable, I will not offer an opinion on that. If you ask me, did Dr. Appel demonstrate that they're inaccurate, I will offer an opinion on that" Tr. 2, 105:8-14. Therefore, for the most part, the testimony by Shamos is a rebuttal of the Appel report.

The sections that follow include testimony offered during three days in March 2009 and information set forth in Shamos' expert report.

B. VOTING SYSTEM STANDARDS AND VULNERABILITIES

To prepare his report, Shamos reviewed the videotaped demonstrations conducted by Appel while at NJSP headquarters, the New Jersey statutes, and the federal voting system standards and guidelines. Shamos also reviewed the Appel report paragraph by paragraph, and spent a few hours with the voting machines in Trenton.

According to Shamos, Appel's report fails to articulate any standard to judge the security of voting systems. Expert Report, ¶ 23, p. 3. He concluded:

> Because no evaluation was conducted of any precinct-count optical scan system, there is no basis in the Report for Dr. Appel's conclusion that New Jersey should immediately implement the 2005 law passed by the Legislature, requiring an individual voter-verified record of each vote cast, by adopting precinct-count optical scan voting equipment.
>
> [Id. at ¶ 24, p. 3-4.]

Shamos recommends that the appropriate response to discovery of any security vulnerabilities is to remediate them, "not to discard a system on which New Jersey has spent tens of millions of dollars and install one that is less secure or whose security properties are unknown." Expert Report, ¶ 25, p. 4

As background for the conclusions set forth in his expert report, Shamos noted:

> If we did a schematic or kind of a flow of how a voting system works, you can see the data is being collected from a voter, and data first has to

> get into the machine so the voter can be prompted. Then at the end of the election, data has to leave the machine and go to some other place where it can be centrally tabulated so the results of the election can be determined. All of this movement of data -- every time data moves there's some chance that it can be intercepted or can be modified, or there's some way of electronically or physically intruding in the system and doing something. These machines all have software in them. Software has to come from somewhere. The software has to be able to be changed because as new versions of the software or firmware develop and are certified, they have to get into the machines so there has to be a way to do that. Well, if there's a way to do it, it means potentially some unauthorized person could also do it because it's physically possible.
>
> And so what I'm looking for are realistic ways in which somebody could usefully tamper with a voting machine and I'm really concerned about the ways in which somebody could do that and not get detected. There are all kinds of mischief you can perform to a voting machine but most of it will be obvious. The real risk is that this will go all the way through to the wrong candidate declared the winner and then it's going to be much too late to do anything about it. That's what I'm really looking for.
>
> [Tr. 1, 38:25-40:5.]

Shamos concluded, based on Appel's standards, that no system could ever be deemed secure. While Shamos acknowledged that many of the vulnerabilities identified by Appel are of concern, he testified that remediation exists to repair the vulnerabilities. In response to questions regarding voting system security vulnerabilities in terms of how they impact the usability of such systems, he noted:

> QUESTION: Do you know of any voting system that does not have security vulnerabilities?
>
> ANSWER: No. Whether in voting or any other field, systems always have security vulnerabilities.
>
> QUESTION: So the presence of security vulnerabilities in a computer system is unavoidable?
>
> ANSWER: Yes.
>
> QUESTION: Should the presence of a security vulnerability bar the use of a voting system?
>
> ANSWER: Depends on what that vulnerability is. It's always a judgment....The opinion is based on a number of factors including how severe is the vulnerability, what is the likelihood of it being exploited, what is the likelihood of the exploit not being detected. And at some point you say it's safe enough and some other point you say it's not safe enough.

[Tr. 1, 94:14-95:7.]

Shamos described security vulnerabilities as falling into two broad categories; (1) physical security having to do with actually resisting physical access to machines; and (2) software security which addresses the possibility that someone can introduce malware into a voting system. According to Shamos, effective administrative procedures are critical to reducing vulnerabilities.

Shamos characterized the Appel approach to security as the "perfection test." Tr. 1, 169-21. In this approach, any security vulnerability whatsoever renders the system unacceptable. Recognizing the impossibility of meeting the "perfection test," Shamos recommends a more pragmatic philosophy: whether or not a specific vulnerability should disqualify the use of a particular voting system. Shamos testified that no voting system could be deemed secure under Appel's standards, because they all have security vulnerabilities.

In commenting upon the significance of Appel's evaluation of the security of the AVC, Shamos criticized the results as not being conducted under real world conditions:

> The significance -- and I think I talked about that extensively in my report -- is that there are all kinds of things you can do to a system when you are allowed complete freedom and an arbitrary amount of time and an arbitrary set of tools and no one to indict you for a crime for doing what you're doing. It's completely different when you're out in the real world. Real world of elections is a suspicious one. The parties are always watching each other. They're very suspicious of everything that gets done even though it may be innocuous. Voters are constantly on the watch. Poll watchers are there. So the things you get away with in a laboratory you do not get away with in real life and so those results of his experience are not directly transferrable to genuine election administration.
>
> [Tr. 1, 106:15-107:5.]

According to Shamos, security vulnerability is a concept separate from accuracy and reliability. "It is true that if there is security vulnerability and the security vulnerability results in someone being able to alter the software, then the software may not be accurate, but the existence of security vulnerability itself has nothing to do with accuracy." Tr. 1, 111:20-25.

In responding to Appel's report, Shamos focused on: (1) physical security issues related to actual physical access to the machines; and (2) software security, related to whether someone can introduce malware into a voting system without the need to bypass physical security interlocks. As to both, he testified jurisdictions can always improve physical and software security.

Additionally, he noted that it is important to distinguish between insider and outsider security threats. Insider threats occur when individuals such as election workers and poll workers, authorized to gain access to voting equipment, undertake unauthorized activities. These insiders normally do not have to defeat regular security measures. If there is a lock, they have a key, or if there's a password, they know the password. On the other hand, outsiders have more limited access, and are deterred by locks, seals, passwords, and machines maintained in locked settings.

C. PATHWAY TO VOTE-STEALING THROUGH THE ROM CHIP

While Shamos acknowledged that the ROM chip is a possible pathway to introduce fraudulent firmware into the AVC, without the source code, a hacker would have to reverse engineer the ROM chip. While acknowledging it is possible to replace the ROM chip with another ROM chip that contains fraudulent firmware, Shamos testified this would be difficult to accomplish in real life. Specifically, Shamos stated:

> [s]o, the issue is the so-called real vote-stealing program, which, by the way, is a hypothetical construct. No one has ever constructed such a thing. They've constructed demonstrations of simple vote-stealing programs. There is no -- I don't have any reason to doubt that the benefit of creating a simple one for the purpose of being able to show to people who are not expert computer scientists how it might be done; that's a fine thing to do. To reason from there, to say that, oh, well, I've done this real simple one, and I can show you by casting three votes that it's counting them wrong, but, if I wanted to be really clever, I could create one that was much more complicated and you wouldn't be able through any testing or any other kind of observation process, ever be able to determine that it was fraudulent. No one has ever done that and, in fact, I have scenarios in my rebuttal report explaining exactly how to detect those things.
>
> [Tr. 1, 124:10–125:12.]

Furthermore, "assuming that a person can easily gain access to voting machines to install this hack, the same is true of the Hursti hack on optical scanners." Expert Report, ¶ 27b, p. 4.

Shamos rejected the notion that fraudulent firmware installed in a machine can remain in the machine and continue to steal votes in election after election. While this might be true if the firmware was never updated with a new version, Shamos represented that firmware updates may occur as often as two to three times per year. When the firmware is updated, the fraudulent program is no longer present in the machine. He further stated that because each election is different from the previous election, the impact of the fraudulent software on future elections could not be controlled. Moreover, "even if true, however, it is equally applicable to DREs with VVPATs and optical scanners." Id. at ¶ 27d, p. 5.

Also, as to repeating the vote-stealing program in election after election, Shamos testified:

> [w]ell, neither he nor anyone else has ever demonstrated that. And, I've explained the reasons that it doesn't make sense. You can't predict the future. You don't know what changes are going to be made, for example, to the ballot structure, either by the vendor or by the jurisdiction. You don't know if the next time you might be getting a Spanish ballot, if you were expecting to see party names in English. Now, all of a sudden, the software isn't seeing party names in English. You just don't know what's happening in the future. So, the idea that this rogue thing sits there for years and years stealing elections is not realistic.
> [Tr. 1, 146:19-147:6.]

Regarding whether anyone has ever verified an attack of a DRE voting system, Shamos testified:

> QUESTION: I believe you testified that you have never in your experience come across a verified attack of a DRE voting system, is that correct?
>
> WITNESS: Well, that's correct, and even the anti-DRE activists concede that there's never been such an incident, nor has there been an incident of an attempt.
>
> [Tr. 1, 134:25-135:5.]

Shamos acknowledged that "if you can get into the guts of the machine, and replace the components with those of your own choosing, you can make the machine do anything." Tr. 2, 9:3-6.

D. PATHWAY TO VOTE-STEALING THROUGH A FAKE Z80

The Z80 is the central processor or CPU that reads the instructions off the ROM chip and performs all the logical operations that the machine performs. In response to a question as to whether anyone has created a Z80 processor chip that can steal votes, Shamos testified that, "no one has ever demonstrated that a fraudulent Z80 chip could successfully masquerade as a real Z80." Tr. 3, 93:14-15. The Z80 by itself doesn't have memory or code. Instead, it takes instructions off of the ROM and executes them. The program is put in the ROM chip and the Z80 will run that program.

E. FIRMWARE VERIFICATION

Shamos noted that one way to detect fraudulent firmware is by firmware verification. The firmware in a machine consists of numerical information that is sitting on the chip. The technician reads every location on the ROM chip to determine whether, bit-for-bit, it corresponds with the version that has been certified. Known as dumping, this process permits the technician to determine whether it is the authorized chip or not. It is true that this kind of check is currently not routinely done, but it can be done, and it makes it easy to detect fraudulent firmware:

> The way you would do the firmware verification is you compute the hash code of what's on the firmware and you compare it to what it's supposed to be as filed by the VSTL during certification. It's a pain, but it's doable, and up until now the vendors have not made it easy.
>
> [Tr. 1, 142:1-6.]

Shamos recommended against performing firmware verification by opening the voting machine and taking out the ROM chip. Besides issues of security, it is important to be able to go to a voting machine and verify the firmware without opening the machine. Instead, a bit-by-bit comparison could be accomplished without removing the ROM chip from the DRE. To accomplish this, the voting machine would have to be equipped with an electrical port to which the technician could connect to a device in order to read the contents of the chip. If the port were provided, it would take seconds. While this port

technology is available, vendors have not included such ports in the DREs. Shamos testified that perhaps an adapter could be added to existing DREs without necessarily requiring the recertification inherent with hardware modifications.

Parallel testing is another process to detect fraudulent firmware. This approach is based on hiring workers on the day of the election to vote on machines set aside at the polling place to evaluate their reliability and accuracy. This type of test is limited to the accuracy of a particular machine. While Shamos testified that Appel's fraudulent firmware could be detected by parallel testing, Shamos acknowledged that he had never performed parallel testing anywhere.[67] In fact, at his deposition, Shamos stated he had invented parallel testing as a joke.

Shamos explained that "in orthodox parallel testing, you remove the machine from service for the entire period that the polls are open, and you cast votes on the machine at the same rate, the same speed as normal voters. And if you do it in the polling place it's easy." Tr. 2, 37:19-25. While counties would have to train workers and purchase additional voting machines to conduct parallel testing on them to ensure that voters aren't waiting in long lines, it is less expensive than throwing out the State's existing election system. In response to a question on cross-examination, Shamos disputed the notion that parallel testing was necessary for a safe election.

On the third day, Shamos testified that parallel testing has been recommended by: (1) the EAC, the official body charged by Congress to advise states on voting procedures; (2) the Brennan Center for Justice of New York University; (3) NIST; (4) the Thornburg Commission; (5) former Attorney General Thornburg; (6) Eric Lazarus, advisor to NIST; (7) the Irish Commission on Electronic Voting; (8) Daniel Castro with the Information Technology and Innovation Foundation; (9) Joseph L. Hall, from the University of California at Berkeley; and (10) Donald Norris, Director of the Maryland Institute for Policy in Research, in testimony before the United States House of Representatives.

[67] He testified that it was used in one county in Pennsylvania and in ten counties in California before they switched to optical scan machines.

Furthermore, the General Accounting Office issued a report in which it found that in 2004, seven states had conducted parallel testing as a useful adjunct to election security**.** Parallel testing has also been endorsed by the Democratic National Committee in a report known as "Democracy at Risk: The 2004 Election in Ohio."

Shamos acknowledged that these organizations have not conducted parallel testing in its pure form. On a scale of one to ten, he said the pure form is a ten, representing, in his judgment, the best parallel testing system. He testified that he does not know of any other organizations or states that have used a system rated at a ten.

When questioned about parallel testing for optical scanning voting systems, Shamos answered that the procedure was not generally recommended.

One last way to detect fraudulent firmware is through checkpointing. Developed in the 1950s, Shamos described checkpointing as a form of parallel testing that does not require removal of a real voting machine from service during an election. While checkpointing is an old concept, he acknowledged: (1) no jurisdiction uses this procedure; (2) election workers would need to be trained; (3) a DRE designed to perform checkpointing would have to go through a rigorous certification process before it could be used; and (4) a vote-stealing program could be detected by checkpointing.

The most successful hack is one that is surreptitiously introduced into the devices that the authorized technicians are using, as testified to by Shamos:

> So all voting machines have a mechanism by which authorized service personnel can upgrade the firmware in the machine. So when they upgrade the firmware, they don't even know that they're upgrading it with malware. And so nothing they would do would be suspicious, they would only be doing what they're normally authorized and supposed to do.
>
> [Tr. 3, 27:13-23.]

According to Shamos, firmware verification is required for the first time under the 2005 guidelines.

F. BUFFER OVERFLOW

When information is input into the computer, the computer places it into memory, into something called a buffer, which is a place where the data is held until processed. All computer programs have a limit on the size of a buffer, with the size determined by the programmer when the program is written. Shamos described the existence of a buffer overflow as bad, but not necessarily fatal, depending where the buffer is located. In addition, software is available to check programs to ascertain whether they have buffer overflow. If there is overflow, it can be fixed by the programmer.

As to comments by Appel, regarding a buffer overflow, Shamos noted:

> [y]es, so, while I agree generically with Dr. Appel that buffer overflows are potential risks, he never ever utilized any buffer overflow that he discovered to show that a single machine instruction in the machine could be altered.
>
> [Tr. 1, 128:23-129:2.]

G. CONNECTION TO THE INTERNET

While WinEDS is not an Internet-enabled program, a WinEDS enabled computer should never be connected to the Internet. In response to statements that this has not been followed in New Jersey, Shamos stated:

> This is a bad and terrible thing. It's never permitted in the states where I do certifications.
>
> So, these machines should never in their lives be connected to the Internet. It's not just, let's disconnect it now and then run the election. It's from day one when it's delivered until it dies you never connect it to the Internet.
>
> [Tr. 3, 153:22-154:14.]

In many counties, election results cartridges are brought to the Municipal Clerk's office and the information is downloaded onto a WinEDS enabled computer. The information is then sent by electronic transmission, through a T1 line or dedicated telephone line, to the Clerk who tabulates the votes. Shamos expressed concerns regarding possible manipulation during electronic transmission unless safeguards were undertaken. Tr. 3, 145:13-14. He noted:

> [w]e in Pennsylvania have actually granted variances to counties who wanted to do it that way provided they made a complete disclosure of the

> architecture of their system and we could assure ourselves that it wasn't susceptible to outside manipulation. So, if it's a dedicated line then we believe that to be sufficiently safe. If their proposal is, I'm going to email it to you over the Internet, no.
>
> [Tr. 3, 157:9-17.]

To avoid the T1 line, the Municipal Clerk could be required to transport the results cartridge directly to the county where the information is ultimately read.

Regarding Internet contamination from a network, including a county's own local area network, Shamos emphasized:

> Well, if at any point in its travels the data that's being transmitted could be interfered with by someone on the Internet, that's not a good practice. And we always require that not only the system that runs the election administration software be dedicated only to that function, but that it never be connected to any network, including the county's own local area network. And the reason for that is that you have no idea who's on the network at the time your machine is connected. They may all be authorized county employees, but you don't know what they're doing or who they've given their password to or whatever. And these machines are cheap, it's just a PC. It's not a waste of resources to dedicate it to this function.
>
> [Tr. 3, 158:20-159:9.]

H. VIRAL TRANSMISSION AND ANTI-VIRUS SOFTWARE

Shamos distinguished between two different viral modes: (1) one from the viral transmission of codes from one voting machine to another through the use of cartridges; and (2) a computer that might itself get infected with a virus that would corrupt the WinEDS program. As for transmission through cartridges, Shamos testified, "you can't have arbitrary people walking up to voting machines sticking cartridges in them and using them to overwrite software." Tr. 1, 152:11-13. Regarding the second mechanism, through WinEDS, Shamos described it as a "terrible thing," Tr. 1, 153:23. As a result, "these machines should never in their lives be connected to the Internet." Tr. 1, 154:10-11. In addition, the WinEDS program should be on a dedicated computer with no other applications running.

Shamos also recommends anti-virus software on a dedicated machine inasmuch as it is impossible to absolutely guarantee that people who are supposed to treat it as a dedicated machine will

actually do so. Therefore, it is important that if someone does connect it to the Internet, even though that may violate a regulation, it still gets detected. One way to achieve this is to remove the network card from the machine, so it's physically impossible to connect it to the Internet. Shamos testified in this scenario, anti-virus protection would not be necessary.

According to Shamos, anti-virus software in almost all cases is provided by a third party. Typically, vendors make recommendations to jurisdictions to acquire third-party anti-virus software. Since anti-virus software is not subject to federal certification, adding it to the computer will not affect the VSTL testing that would have occurred.

I. ENCRYPTION

In the AVC, the results cartridge and the four flash memory chips should be encrypted. Tr. 3, 151:23-152:12. Shamos described this as a "small matter of programming" and represented that "other vendors do it." Tr. 2, 134:2-5. In fact, he said, "it's commonly done in the industry." Ibid. The current 2005 guidelines require encryption. In response to a question from the court, Shamos testified, "you can't encrypt the ROM chip because the ROM chip itself contains the instructions that are going to be used in the machine." Tr. 2, 133:2-4. Furthermore, WinEDS does not use encryption. When asked whether a system using new encryption software would have to be reviewed by the ITA, he responded:

> [y]es. We're dealing with - - when you encrypt this information, we're dealing with critical information relating to votes and that's the heart – the beating heart of the whole system and it has to be looked at.
>
> [Tr. 3, 155:19-22.]

In response to questions regarding what election officials should rely on for the official results of an election, Shamos testified it should be the actual tape that comes out of the voting machine; that "there are human beings that have viewed it and signed it and authenticated it." Tr. 2, 130:20-22.

J. ADVANTAGES OF THE DRE OVER OTHER SYSTEMS

One of the benefits of DREs is that they make multiple identical copies of the choices made by the voter. This is a feature not available in document ballot systems. As explained by Shamos:

> [s]o you have multiple copies of the voter's choices. You have four inside the flash memories in the Advantage. You have one on the results cartridge. There are four chips that comprise the flash memory. The benefit is, additionally, that because the results cartridge is removable, once it is removed, then any alteration to the results cartridge cannot change anything that's on the flash memories in the machine, and vice versa.
>
> If someone gets access to the machine, changes the results in the flash memories, that will not change either the printout that was made on election night at the polling place or the results on the results cartridge.
>
> So there's security achieved by separating these things immediately upon the close of polls. If somebody manages to alter the results in a results cartridge, and there is reason to suspect that this has happened, then you can always go back to the flash memories on the machine, print out a new summary total, or actually read out the memories completely. In addition to reading out the audit trail of the cast vote records, you can determine whether an alteration has been made to the results cartridge.
>
> [Tr. 3, 110:19-111:16.]

The flash memory is in the machine and permanently mounted on the motherboard. If the results cartridge is lost, the results can be recreated by dumping the information on the flash memory. According to Shamos, results cartridges are lost with some degree of frequency. Tr. 3, 115:23

Therefore, a DRE has a results cartridge, flash memory, a results summary print out produced by the software at the end of voting and the audit trail of the individual cast vote records. Tr. 3, 116:15-23. The cast vote records compare the total number of people who voted with the number of votes cast. A cast vote record is a complete snapshot of how an individual voter voted, but it's not connectible with any one particular voter.

K. VVPAT OR OPTICAL SCANNING SYSTEM

Shamos testified, "it's okay for a machine to have voter-verified paper trails. It's just not a requirement that they have voter verified paper trails." Tr. 2, 78:13-16. On the third day of testimony, the discussion of the VVPAT continued:

> COURT: And is that because you testified that the sequential and the cut-and-drop have, in your judgment, have problems?
>
> WITNESS: Yes.

COURT: If there was a -- is it possible that there could be a VVPAT that met all your requirements?

WITNESS: Oh, I think it's possible that there could be. No one has designed one yet.

COURT: I see. So your current objection to the VVPAT is the existing technology?

WITNESS: Yes.

COURT: Not to the concept?

WITNESS: I don't mind voter verification. If it can be achieved properly through paper, that's fine. If it can be achieved properly through some other means, that's fine, too.

[Tr. 3, 67:10-68:1.]

Shamos also expressed the opinion that DREs are not improved by any currently proposed paper trail method:

COURT: DREs are better without the current paper trail mechanism?

WITNESS: Yes. I don't know of a current paper trail mechanism that would make the DRE better than a DRE without a paper trail. But I don't rule out the possibility of a better design that might make for a very effective paper trail machine, and I wouldn't be against it. . .

[Tr. 3, 82:5-12.]

***

WITNESS: All voting machines, except lever machines, can be audited. The way you audit a DRE.

COURT: A DRE without a VVPAT?.

WITNESS: Without a VVPAT.

COURT: I guess you compare the counter?

WITNESS: The way you audit it is you take the cast vote records, and tabulate them separately and see if they correspond to the totals produced by the machine.

COURT: I understand that. So it audits the machine in terms of the number. It doesn't audit the machine in terms of whether the votes went to the right parties?

WITNESS: Correct.

COURT: Right.

WITNESS: In any system that has audits, whether it's voting or not, you have to verify the integrity of the auditing mechanism.

COURT: Right. Okay. But you can do that independent of whether there's a VVPAT or not? You don't need a VVPAT in order to audit the machine?

WITNESS: Correct.

COURT: You can do it without?

WITNESS: Right.

COURT: In your opinion, should there be, even without a VVPAT, some audit review?

WITNESS: Yes.

[Tr. 3, 85:21-88:3.]

Shamos does not support a cut-and-drop VVPAT system. In his judgment, "the fundamental problem with the cut-and-drop system is that it is essentially impossible to certify after the election that one of these cut sheets actually was cast and verified by a voter during the election. It's one of the small advantages that the sequential VVPAT has." Tr. 2, 70:14-21. Most states that utilize a VVPAT do not use a cut-and-drop system. Based on current designs, Shamos testified that DREs are better without the currently available paper trail mechanisms. Tr. 2, 81:25-82:1.

When comparing security vulnerabilities of DREs and precinct-based optical scanning voting systems, Shamos testified, "in general it's much easier to tamper with optical scanners, they're much simpler than DREs. They don't have to make a presentation, a visual presentation to the voter the way the DREs do . . ." Tr. 2, 47:6-9.

While Appel recommended that New Jersey adopt precinct-based optical scan machines, Shamos testified that Appel did not conduct any security study or review of the vulnerability in optical scan systems. As for precinct-based optical scanners, there are problems with lost ballots, finding more ballots

than voters, and other irregularities. Shamos represented that there are no uniform procedures for the collection, guarding, and storage of ballots.

According to Shamos, many of the vulnerabilities Appel identified in the AVC are far worse in optical scan systems. One problem is how to handle a recount in an optical scan election. While Shamos has recommended certification of precinct-based optical scan voting systems, he noted that this system also has security vulnerabilities that must be remediated. Shamos discussed difficulties with using precinct-based optical scan voting machines, also described as document ballot systems. For example, Shamos asked what process should be employed to conduct a recount: (1) recount the ballots on the same machines they were counted on; (2) recount on a different machine; or (3) conduct a recount by hand. Since only one copy of the voter's intent exists, what occurs if anything happens to that copy? Furthermore, when individuals handle paper ballots, there is always the possibility for ballots to be changed, substituted, or discarded. Finally, Shamos pointed out that optical scan ballots result in a large percentage of deviant or unclear marks made on the ballot, sometimes making it impossible to make a determination as to whom the voter voted for, or intended to vote for.

When asked whether DREs interpret the voters' intent better than optical scanners, Shamos replied, "oh, absolutely, because the choice on a DRE is binary. You either have selected the candidate or not. There's no intermediate position as there is on an optical scan vote." Tr. 3, 139:18-21.

As to security vulnerabilities with optical scanner machines, Shamos testified that the firmware in the optical readers can be corrupted and there are a number of manipulations that technicians who maintain the scanners can perform. Firmware can be replaced the same way as on the DRE. This can be achieved by changing the chip or when the technician updates the firmware in the optical scanner. Furthermore, electrical manipulations are easy to perform. One can adjust the sensitivity of the optical reader so that marks are slightly off of the absolute black requirement. There are also manipulations that the contractor, who actually prints the ballots, can perform.

As to the possibility of lost ballots, Shamos represented that in every election cycle in the United States in which optical scan voting machines have been used, ballots have been lost. Furthermore, optical

scan machines cannot be effectively audited. If the original ballots have been altered, lost or replaced, no audit is possible because the optical scan system provides only a single record of the voter's choice. To emphasize this point, Shamos noted:

> In 2004, three weeks after the election in San Francisco, ballot boxes were found floating in a San Francisco bay with wet ballots in them that obviously had not been counted. So there's nothing inherently more secure about optical scan systems than there is with DREs.
>
> [Tr. 3, 78:17-22.]

L. STANDARDS FOR SECURITY

Security, in the context of electronic voting systems, refers to the resistance of a system to deliberate penetration by outsiders, including both physical tampering and software tampering, which affects the correctness of the vote totals. It is completely separate from accuracy and reliability.

Regarding tamper-evident seals and locks, Shamos testified:

> Tamper-evident seals don't prevent people from breaking in. Tamper evident seals are designed for allowing us to determine that a break-in has occurred, also to make it more difficult for somebody to achieve a break-in, and also to serve as a warning to the person. Each step somebody has to take further into crime gives him a chance to review his action and possibly not engage in it.
>
> [Tr. 3, 101-3-10.]

During the trial, several lay witnesses testified that results cartridges are brought to municipal clerks or satellite offices and placed in a cartridge reader. The results are then transmitted through a T1 line to the Clerk's office. To ensure the safety of this method, Shamos testified that in Pennsylvania, the Secretary requires that no voting information may be transmitted by Internet or network unless certain conditions are followed. Further, the election district/county is required to provide full disclosure of what the architecture is and the proposed configuration to determine whether it poses a risk.

M. SOFTWARE INDEPENDENCE

Software independence is a term created by the TGDC of NIST. Shamos testified that "software independence is, by itself, a wonderful principle." Tr. 1, 161:7-20. What software independence is designed to do is exactly what its definition says, that is, to assure that an undetected change in the

software will not cause an undetected change in the outcome of the election. Software independence achieves that. There are many different ways of accomplishing software independence.

According to Shamos, software independence is not required under the existing set of federal guidelines. While mentioned in the draft report for the next VVSG and recommended by the TGDC, the EAC rejected the recommendation.

N. CERTIFICATION AND SUNSET PROVISIONS

Shamos testified the ITA came into being along with the promulgation of the 1990 standards. Shamos confirmed that the 1990 standards, 2002 standards and 2005 guidelines are voluntary. Even in elections for federal office, HAVA does not require adherence to any federal standards or guidelines. New Jersey has not adopted the standards or guidelines.

In response to questions regarding ITAs, Shamos described them as "pretty good for the tests that they do." Tr. 1, 167-7-8. While supporting the notion that each voting system should be required to undergo standardized testing for accuracy and reliability, Shamos noted the ITA process has limitations: (1) it's not open; i.e., there is no sunshine; (2) it only does tests associated directly with the standards; and (3) many voting systems pass ITA tests that shouldn't.

In response to the question of whether the 1990 standards only test hardware and not software, Shamos responded:

> I don't - - that's not accurate. The - - it's impossible in a voting system to test hardware without testing software. The hardware was run by the software. And so there were functionality requirements in the 1990 standards, which, if they fail, would imply a software failure.
>
> [Tr. 1, 192:8-13.]

The 2005 guidelines are the newest set of guidelines. According to Shamos, the 2002 and 2005 standards test the source code and are much more stringent than the 1990 standards. Shamos testified that "New Jersey should adopt more stringent security guidelines." Tr. 1, 186:24-25. He agreed with Appel that certification of one version should not provide confidence in the security and accuracy of a different version.

When software is updated, it may or may not require recertification. "If the change is purely cosmetic, for example, changing the font size on the display of the machine, that's typically something that's not going to require recertification. If there's anything that gets anywhere near the handling of votes or the tabulation of votes, certainly recertification is needed." Tr. 3, 150:19-25.

Shamos supports sunset provisions for voting machine certifications so that the certification of a voting system, at a given moment in time, does not continue into the infinite future. Many modifications are added to the VVSG because of vulnerabilities that have only become apparent in the recent past.

O. STORAGE AND LEAVING MACHINES AT POLLING PLACES

Appel and Shamos agree that the practice in many New Jersey counties of leaving voting machines unguarded at publicly accessible locations for a week or more prior to an election increases the risk of tampering with the machines. As for the tamper-evident seals, he testified, "tamper-evident seals don't prevent people from breaking in. Tamper-evident seals are designed for allowing us to determine that a break-in has occurred, also to make it more difficult for somebody to achieve a break-in, and also to serve as a warning to the person." Tr. 3, 101:3-8.

Shamos testified that the practice of election districts leaving machines unattended at polling places for weeks, before and after elections, is widespread across the country.

P. DISAGREEMENT BY SHAMOS WITH APPEL

To summarize, Shamos disagrees with Appel as follows:

(1) Appel did not use any of the federal guidelines for voting systems in reaching his conclusions;

(2) the term "accuracy" as used by Appel is his personal definition;

(3) Appel's evaluation of the AVC's accuracy does not even minimially comport with the standards and methodology used in the trade, federal guidelines, or statute;

(4) Appel did not define "security," "accuracy," or "reliability;"

(5) Appel failed to establish that the AVC does not meet the federal guidelines or HAVA requirements for accuracy;

(6) there is no requirement that any component of a voting system be absolutely immune to tampering;

(7) there has never been a verified attack of a DRE in the United States since its first use in 1979;

(8) there has also never been an incident of an attempted attack on a DRE;

(9) creating vote-stealing fraudulent firmware is a difficult task fraught with technical barriers;

(10) fraudulent firmware cannot avoid suspicion or detection;

(11) fraudulent firmware cannot operate in future elections;

(12) ROM chip manipulation is not a realistic risk;

(13) viruses are not a legitimate risk;

(14) the daughterboard virus that could spread is fictional;

(15) the Z80 chip manipulation is not a legitimate risk;

(16) WinEDS manipulation does not affect official results;

(17) results cartridge manipulation does not affect official results;

(18) firmware verification can be done;

(19) there is no evidence that the AVC, when not hacked, has design flaws that cause votes to be lost;

(20) the AVC indicates under-votes and satisfies the 2002 federal guidelines which do not even apply in New Jersey;

(21) the complaint that a poll worker can peek through slits in the AVC while a voter is voting is ludicrous;

(22) the AVC permits write-in votes to be changed after pressing "enter," but before pressing the "cast vote" button;

(23) paper trails are not necessary for a safe election;

(24) it is much easier to tamper with paper vote records than electronic vote records;

(25) it is not easy to replace the firmware in the AVC. Under artificial conditions, Appel was able to replace the firmware. That is a very different thing from injecting fraudulent software into a real election and having it go undetected;

(26) precinct-based optical scan voting systems are not more secure, more accurate, more reliable or more auditable than DREs without VVPATs;
(27) it would be inappropriate to discard New Jersey's voting systems and install a precinct-count optical scan system that is less secure;

(28) it is not well known how to design a vote-stealing program so that it can avoid detection. No one has ever done that;

(29) the statement by Appel that it is well known how to design a vote-stealing program so that it can avoid detection is preposterous;

(30) no one can defend itself against parallel testing;

(31) the manipulation described by Appel can also be performed as well on optical scanners; and

(32) the statement by Appel that cleverly designed fraudulent firmware can detect differences in the patterns of use between testers and real voters is untrue. There has never, ever been a paper written on what the voting patterns of real voters are.

While acknowledging that changes should be made, Shamos testified that remediation is available and challenged the notion that New Jersey should abandon the current AVC.

With reference to the findings by Appel, Shamos testified, "I think everybody in the voting field should be concerned about Appel's findings. I think the findings should be evaluated and necessary changes to voting software and physical security and administrative procedures should be done." Tr. 3, 9:22-10:1

Q. AGREEMENT WITH APPEL

On cross-examination, Shamos agreed with Appel that New Jersey should adopt more stringent security guidelines. He noted:

(1) the plastic strap seals only provide a veneer of tamper protection;

(2) the locks and seals don't prevent tampering, they delay tampering;

(3) the code of the AVC does not follow the best software engineering practices;

(4) the audio-ballot cartridge is one way to attack the motherboard;

(5) the computer on which WinEDS runs should never at any time in

its life be connected to the Internet;

(6) anybody who gets direct access to the machine unobserved can pollute WinEDS

(7) the audio-ballot cartridge that is fed into the daughterboard is a viable mechanism of infecting the votes;

(8) machines now in use in New Jersey are insufficient to detect fraudulent software;

(9) through reverse engineering one can create fraudulent firmware;

(10) it is possible to reverse engineer ROM chips that are used in the AVC to create vote-stealing programs;

(11) the software design practices for the AVC advantage are poor and in need of improvement;

(12) New Jersey's procedures are inadequate for detecting security flaws;

(13) examiners should spend days on the certification process;

(14) software should be examined by computer experts during the certification process;

(15) ITAs came into use following the issuance of the FEC's 1990 guidelines regarding DREs;

(16) the 1990 guidelines were made more stringent in 2002 and 2005;

(17) a few states have adopted the 2005 guidelines;

(18) New Jersey should adopt stronger security guidelines;

19. the 1990 standards do not require an examination of DRE software and source code to determine if it is flawed;

(20) the option switch bug is bad;

(21) it would be easy to create fraudulent firmware that does not cheat in the Pre-LAT mode;

(22) it would be easy to design fraudulent firmware that does not steal more than 20 percent of votes in a particular precinct;

(23) it would be easy to design fraudulent firmware to refrain from cheating until at least 150 votes are cast;

(24) it is possible to design fraudulent firmware that assures candidate totals are not greater than the public counter;

(25) the data on the results cartridge should be encrypted; and

(26) the interface can contribute, under certain circumstances, to a voter being confused. However, it is remediable.

R. TITLE 19 COMMITTEE

In response to questions from the court regarding the appropriate number and qualifications of members of a state certification committee, Shamos testified the Committee should consist of: (1) a member with at least an undergraduate degree in Computer Science, with professional work experience in computer architecture, the security vulnerabilities of computer systems, hardware, and software, who understands voting system manuals and ITA reports; (2) a member familiar with and who has professional experience in election administration processes and procedures; and (3) a member familiar with and with experience in election codes of the state.

14. PAUL DAVID TERWILLIGER(WITNESS FOR THE STATE)

A. BACKGROUND

Terwilliger received Bachelor of Science and Master of Science degrees in Electrical Engineering from the Massachusetts Institute of Technology ("MIT") in 1982, as part of a cooperative five-year work-study program. The program focused on electronics, microprocessors, firmware, and software. In 1989, he obtained a Master's degree in Business Administration ("MBA") from New Hampshire College.

After graduating from MIT, Terwilliger worked for a year-and-a-half as a senior engineer for Sanders Associates, concentrating in the areas of microprocessors, circuitry, analog circuitry, and writing software and firmware. After leaving Sanders Associates, Terwilliger worked three years for Cadec Systems ("Cadec") as a senior engineer. At Cadec, he focused on product development, microprocessor design, analog and digital circuitry, and writing software and firmware for on-board computing systems for trucks and trucking fleets. After leaving Cadec, while pursuing an MBA, Terwilliger worked for Enterprise Systems ("Enterprise"), developing new product lines and hardening standards for computers.

After leaving Enterprise, Terwilliger worked approximately one year for Datasec Corporation as a program manager. In this position, he developed products and product modifications, and was involved in the military's Tempest standard to harden computers to prevent eavesdropping. Next, he worked for Circuits and Systems ("Circuits") as a senior engineer, where he developed firmware and wrote source code for the AVC. At the time, Circuits had a business relationship with Sequoia.

When Circuits went out of business, Terwilliger and Circuits founder Drew Sunstein co-founded Sunrise Labs. Sequoia became their first client. As Vice President of Sunrise Labs from January 1992 to February 1997, Terwilliger continued to work on the AVC and, at some point, transitioned from writing the majority of the source code to working on new features to be implemented and testing them afterwards. In reference to the initial version of the AVC, the following questioning occurred:

> QUESTION: When you first got involved with the Sequoia Advantage, what versions of the Sequoia Advantage voting machine did you start with?
> ANSWER: The first one that I contributed anything to was version 2.13.
>
> QUESTON: And what version is it that you actually had - - what version did it arise to when you actually had hands-on experience with?
>
> ANSWER: The last one that I was responsible for doing all of the firmware for was version 7.00F.
>
> QUESTION: What percentage of the firmware were you personally responsible for in versions 2.13 to version 7.00F?
>
> ANSWER: Virtually all of it, at least 99 percent.
>
> [Tr. 17:7-20, Mar. 30, 2009.]

Terwilliger also contributed to design and source code development of both Versions 8 and 9.00H. As to Version 9.00H, he testified:

> QUESTION: Now, in relation to version Advantage Version 9, what role did you specifically play in the development or design of that voting system?
>
> ANSWER: Well, specifying how it worked. Again, Version 9 was when the audio-voting was introduced, and so, specifying how that should work, the details, you know, the user interface, the voters' interface, so when they press buttons, what happens. Specifying how the

> format of the ballot definition needed to work with that. I was also testing that firmware as it was developed.
>
> [Tr. 18:9-20.]

From March 1997 until April 2007, Terwilliger was responsible for ensuring that Sequoia products met FEC and EAC standards. While having no involvement in the original AVC electrical design in 1986 and 1987, he worked on it in 1991 and was involved in the major redesign in 1994 with a new CPU board. Involved in the certification process from 1994 to 2007, he testified, "I was involved in the various certifications of the Advantage, taking it through that process starting with the first time it was certified which I think was in 1994, or maybe 1995, all the way up through 2007." Tr. 21:13-17.

Terwilleger left Sequoia in April 2007 to engage in private consulting. Since May 2007, Terwilliger has successfully completed several contracts for Sequoia as a consultant, in the areas of patent and intellectual property, product modifications, and writing code for firmware development. After writing code, it is then transmitted to Sequoia through E-mail over Sequoia's virtual private network ("VPN"). Terwilliger has a password to access the system, and also a VPN token that requires the user to type in additional unique numbers.

Terwilliger has never testified as an expert witness, held any academic appointments or published articles. While not a licensed professional engineer and does not possess a degree in Computer Science or Computer Engineering, he has eighteen years of experience working on the development of the AVC Advantage and AVC Edge, along with fifteen years experience interacting with the FEC and EAC regarding the certification of Sequoia products.

Terwilliger is trained and experienced in reading and writing in "C" language, the language in which the majority of the firmware in the AVC is written. As a graduate of MIT and the University of New Hampshire, all of Terwilliger's work experience has been in the fields of project development, the design of microprocessors, analog and digital circuitry and developing and writing firmware and source code.

The court permitted Terwilliger to testify as an expert in the AVC and the voting machine certification process. N.J.R.E. 702.

Terwilliger co-authored a report, dated October 2, 2008, with Edwin Smith and Michelle Shafer ("Shafer"), both employed by Sequoia. Smith holds the position of Vice President of Compliance, Quality, and Certification, and Shafer is the Vice-President of Communications and External Affairs. Terwilliger issued a supplemental report, dated February 19, 2009, in response to certain alleged anomalies or insecurities of the AVC as set forth in a letter, dated February 3, 2009, from counsel for plaintiffs.

B. THE AVC ADVANTAGE

The AVC is an example of a DRE in which voters make selections on an interface panel that confirms that the voters' choices have been registered by the machine. It also creates multiple copies of the vote in the machine's redundant memory. So, if there is a failure in the components, there is a backup record.

The AVC has several different operating modes. Maintenance diagnostics is essentially the machine's idle mode. In this mode, memory tests are conducted and auxiliary reports can be printed. Auxiliary reports are generated when a machine checks the results cartridge to print a report or post events to the internal logs, which are where any significant actions are recorded for subsequent review. In this mode, there's no ballot definition, that is, no election loaded on the machine. As to a question regarding "what the results cartridge is," Terwilliger testified:

> That's a removable memory device that starts out holding the ballot definition data for the election, and it's one of the memories where the votes are stored while voters are voting.
>
> [Tr. 46:17-20.]

In response to questions on direct-examination, Terwilliger explained information contained in the auxillary reports. He noted:

> That's a feature that has been in the machines forever, so that a machine that's not being used for an election could be used to check the contents of another results cartridge or to print a report from it – for whatever

purposes might be needed.

QUESTION: In the auxillary reports, are events posted to the internal logs?

ANSWER: Yes. For any significant action on the machine, whether it's testing memory, printing a report, or loading a ballot, for instance, the internal logs do that.

[Tr. 46:23-47:8.]

Regarding the significance of the information obtained from the internal logs, Terwilliger testified:

[s]omeone can go back later and review the activity on a machine.

QUESTION: What type of activity on the machine would be revealed on that?

ANSWER: Well, for example, in the maintenance test, the technician might be tasked with doing or actually done, that they passed. Or that someone had been perhaps trying to tamper with the machine, experiment with it you would see extra events in that log.

QUESTION: How would that - - how would the internal log indicate that somebody attempted to tamper with the machine?

ANSWER: It might show additional power on or power off events. It might show attempting to load a ballot at some time when the jurisdiction was not in the process of preparing machines for an election.

[Tr. 47:9-48:1.]

As part of maintenance diagnostics mode, one of the options is to prepare the machine for an election by loading the ballot definition. Terwilliger described ballot definition as the collection of data files that define the details of the election. This includes the offices in the race, the names of candidates, the number of candidates to elect for each office, and the positions of the candidates on the ballot. After the ballot information is verified, the technician tests to make sure the machine is operating correctly and that the ballot definition has been properly loaded. Each additional mode includes different tests for accuracy at different stages during the voting process.

Upon completion of this, Pre-LAT allows the technician to again test the correctness of the ballot. In Pre-LAT, the machine casts and tabulates test votes to verify its proper operation. In response to

questions on cross-examination, Terwilliger testified that malware may be present on a voting machine but not appear during a Pre-LAT test.

The post-election logic mode ("Post-LAT") conducts tests when there has been an accusation of machine malfunction following the completion of an election. "Between voter test mode" is a function that tests the voter panel, implemented in response to concerns that a machine may not react after a voter makes his selection. The machine can be put into this mode in between voters during an active election and will verify whether the voters' choices registered with the machine. If there is a failure in the vote-saving process, a "System Error 31" message appears along with a number that indicates during which step of the process the failure occurred.

As noted heretofore, every machine contains a "results cartridge," which is a removable memory device that holds the ballot definition data for each election. Memory is also stored on the motherboard in the form of internal, battery-backed RAM. The results cartridge and the motherboard combine to make up the "redundant memory." If a results cartridge is lost, damaged, or malfunctions, the results can still be retrieved from the internal memory by conducting an "audit trail transfer." This is a software dependant process in which the electronic information is transferred from the internal memory to a special cartridge. When reports are printed, the reports disclose what source of memory they're being printed from. The basic AVC does not use flash memory. Flash memory is only on the audio-subsystem support.

There are four methods to store votes within the AVC. First, when the voter presses the "cast vote" button, a ballot image is stored. Second, summary totals are kept for each candidate. When a voter receives a vote, the counter for that candidate is increased by one. Third, the data is stored redundantly in the internal memory and on the results cartridge. Fourth, counters are maintained for the option switch counts, used in primaries.

Regarding the operation of the machine, "vote data is written to the results cartridge after each voter and at all times the internal memory and results cartridge storage must be identical or the machine will halt." Report, § 2.5, p. 3.

Terwilliger described the different behaviors of the AVC when it is in the activated state as

opposed to the deactivated state. “When a machine is activated for voting, there is a sound that’s played, and the booth light is illuminated. Depending on the configuration option, the lights next to each of the contests that the voter is eligible to vote in would illuminate.” Tr. 58:20-24. After the voter makes the first selection, the “cast vote” button will light up and remain on until it’s pressed. The candidate names are on the printed ballot overlay. When the voter begins to press buttons next to the candidate names, there is a confirmation in the write-in display to signify that the candidate has been selected or deselected. Each candidate name selected remains illuminated until the voter has completed voting and presses the “cast vote” button.

When the “cast vote” button is pressed, the machine plays the same musical tone to indicate that the voting process is completed. As described by Terwilliger:

> Well, the cast vote button is - - the illumination is turned off, all of the lights on the voter panel representing the voter selections are turned off, the booth light is turned off, and the vote is saved to the redundant memories, both the internal memory and the results cartridge.
>
> [Tr. 61:21-62:1.]

On cross-examination, Terwilliger testified he had not conducted any studies in terms of the audible sound being easily heard. He noted, however, that he had personal experience listening to the sound from visiting polling places during elections and not noticing any confusion by voters or complaints by poll workers. The issue of under-votes was also raised:

> QUESTION: Do you agree with Professor Appel that the AVC does not alert the voter that they may have voted or may have not voted for offices on a ballot?
>
> ANSWER: It depends on whether the configuration option for turning on the light by the contest header, whether that configuration is used or not. In the case where it is not used, where that light is not illuminated, then the voter is not alerted.
>
> QUESTION: So it depends?
>
> ANSWER: Yes.
>
> [Tr. 59:22-160:7.]

Sequoia designed the Advantage with "personal choice" capabilities, in compliance with New Jersey's method for allowing a voter to write in a name that is not on the ballot. The AVC has a selector for personal choices. After pressing the selector, the voter then types in the name of the candidate on the keyboard underneath the voter panel. If the voter wishes to change the name after pressing "enter," a poll worker must reset the machine to get a fresh ballot. This is possible so long as the voter has not pressed the "cast vote" button. Once this button is pressed, the vote cannot be changed.

C. CERTIFICATION OF AVC TO FEDERAL STANDARDS

Terwilliger testified that when the AVC was originally designed in 1986-1987, there were no federal standards, so it was designed to meet the specifications set by Sequoia. The FEC released the first government standards in 1990. At this time, the standard test for accuracy was whether a machine counted 297,000 votes (give or take) without error. The first time Sequoia presented the AVC for federal certification was between 1994 and 1995. The AVC passed this test and became certified to the 1990 standards.

Terwilliger also testified to contributing to several AVC upgrades. While Version 9.00H is not certified to the 2002 standards, in 2005, Sequoia applied to certify the AVC D-10 to the 2002 standards. The 2002 standards required changes to the way software is written and also addressed accessibility and audio-voting. Sequoia certified the AVC D-10 according to the 2002 standards in 2005. Sequoia has yet to obtain 2005 certification for the D-10. Any changes made to comply with the 2005 standards will, in all likelihood, result in a new model, the D-11.

The D-10 includes an option for VVPAT. When Sequoia added audio-voting to the Advantage, it had to add additional memory to store the audio data; thus it developed the "daughterboard" to increase the memory capability. Upgrading the AVC Version 9.00H to a D-10 would require the installation of additional flash memory to the daughterboard. Terwilliger testified the D-10 has been employed on a small scale in the past winter's election. It is not currently used in any other states, though other states employ the Sequoia Edge with VVPAT.

In response to questions from the court relating to the difference between the Version 9.00H and the D-10, Terwilliger explained: (1) the AVC D-10 encompasses the additional coding requirements that relate to how software is actually written and documented; (2) the D-10 is available with or without a VVPAT; (3) the D-10 is certified to the 2002 standards, which became effective in 2007; (4) if the D-10 were to be certified to the 2005 standards, it might be called a D-10 with a new firmware number, or become known as the D-11; (5) if certified to the 2005 standards, the AVC would be required to go through the VSTL; (6) changing the AVC Version 9.00H to a later version would require updating the software; and (7) changing AVC Version 9.00H would require changing the hardware, since the "audio subsystem now becomes the main intelligence of the machine, and the original CPU board which has the Z80 on it, is just handling some of the user interface components." Tr. 107:22-25.

In response to questions by the court, it became apparent that the new and improved Version 9.00H equipped with the new firmware is, in fact, the D-10, with one variation. The D-10 operates what has been called the audio subsystem. This means that the daughterboard is now the main intelligence of the machine, and the original CPU board that has the Z80 on it just handles some of the interface components. This modification was necessary because the Z80 processor board and its memory did not have the capability to store the audio data. The motherboard, previously the main processing unit, has become essentially an appendage. As a result, the newer machine has made the daughterboard the equivalent of the motherboard.

In response to the court's inquiry as to whether it would require both software and hardware modifications to make the Version 9.00H into a D-10, Terwilliger stated:

> WITNESS: Yes.
>
> COURT: And both of those would be required to go back and be re-certified by ITA?
>
> WITNESS Sequoia has already done that and it has gone through that process.
>
> COURT: Well, we're talking about taking the existing machines and updating the firmware and making the modification to the hardware?

WITNESS: Yes, and that configuration with those modifications has already gone through the ITA process.

COURT: And that would be the D-10?

WITNESS: Yes.
COURT: But we're using 9 machines, you'd have to update the firmware?

WITNESS: Yes.

COURT: Okay. And you're saying that firmware has already been approved by the ITA?

WITNESS: Yes.

COURT: And installing it onto a different machine makes no difference?
WITNESS: Well, these are the equivalent machines. You do have to make that hardware modification to the audio daughterboard.

COURT: And that wouldn't require going before the ITA?

WITNESS: It's already been done.

COURT: On a D-9?

WITNESS: Yes, that was the configuration of the ITA testing.

[Tr. 111:11-112:15.]

D. SUPPLEMENTAL REPORT

While Terwilliger agrees with Appel that a FPGA can be made to act like a Z80, he noted:

> [t]he plaintiff's Expert Report then makes a huge leap, from implementing what is merely a counterfeit Z80 to implementing a counterfeit Z80 with embedded fraudulent firmware. I envision many technical obstacles, such as pretending to access instructions from the ROM chips while secretly executing other firmware even when being observed, perhaps by a logic analyzer.
>
> [Supp. Report, ¶ 5.3, p. 6.]

Terwilliger disputes the notion that vote-stealing computer viruses can infect the AVC and propagate through the AVC. Appel Report, §§ 20-21. Even Appel recognized that the only firmware that might be affected is that of the audio subsystem, and that a very small number of votes are cast using

audio. Furthermore, plaintiffs presented no evidence to establish that a virus can infect the firmware that controls the AVC itself – only the audio subsystem. Expert Report, ¶ 7.1, p. 12. According to Terwilliger, the current version of the AVC firmware, D-10, now certified by the State of New Jersey, has already addressed this issue. Expert Report, ¶ 7.3 p. 12.

Terwilliger noted that, while the laptop from Union County does not conform to Sequoia's guidelines, "plaintiffs have not described how a WinEDS computer properly configured and hardened against known Windows vulnerabilities is at all vulnerable." Report, ¶ 8.2. p. 13. Furthermore, Terwilliger testified that Appel's reliance on the California Top-To-Bottom study, conducted in 2007 regarding security vulnerabilities in WinEDS 3.1, is misplaced. Specifically, the version of WinEDS in New Jersey is newer than that studied by California and the later version addresses the issues raised during the California review. Expert Report, ¶¶ 10.1-10.2, p. 13.

Regarding fleeing voter policies, Terwilliger testified the plaintiffs failed to establish any nexus between a fleeing voter and an insecurity or inaccuracy of the voting machine. Furthermore, he rejects claims that: (1) cartridges used in the AVC are vulnerable to having wireless systems installed to manipulate contents; (2) fraudulent intelligent results cartridges could steal votes; or (3) electronically-stored "ballot images" compromise the privacy of ballots.

E. REVERSE ENGINEERING

Terwilliger does not challenge the fact that Appel's team of students reverse engineered approximately twenty percent of the AVC firmware:

> QUESTION: And if Dr. Appel or his students were able to reverse engineer 20 percent of the code, is it fair to say that with a little more time they could have reverse engineered the whole thing?
>
> ANSWER: Going from 20 percent to a hundred percent does take more than a little more time; it sounds like maybe it's five times as much.
>
> [Tr. 90:14-19.]

In the joint report, Terwilliger questioned the success of reverse engineering in the real world, by stating:

> Significantly, they fail to mention that they cannot put the reverse-engineered code back into the Advantage or would do this after describing in great detail how they could reverse engineer the firmware. Without a method for successfully re-installing the reverse-engineered firmware, this reverse engineering exercise is a waste of time. During the investigation/classroom experiment that produced their report, the academics relied on compilers and other tools provided by Sequoia. It took Sequoia engineers two weeks to make ready and provide these tools to the academics. The academics also failed to account for new product introductions by Sequoia. New voting machine software is typically introduced to the marketplace every year or two. New voting machine firmware would lay waste to any reverse-engineering program.
>
> [Joint Report, § 11, page 8.]

Furthermore, ROM chips are tested as part of the process for setting up for elections and operating the machine. Terwilliger did not know, however, whether New Jersey tests ROM chips to check for evidence of tampering. On cross-examination, Terwilliger agreed with Appel's conclusions that fraudulent firmware can steal votes and that ROM chips can be easily replaced.

F. OPTION SWITCH BUG

Terwilliger testified that an "option switch error" occurred in a primary election only if a poll worker inadvertently pressed the wrong button. To remediate the problem, Terwilliger drafted a technical description of the option switch issue, provided a narrative of the problem and designed a solution. According to Terwilliger, the problem has been eliminated in the D-10 software.

15. ROGER GLENN JOHNSTON, Ph.D. (WITNESS FOR PLAINTIFF)

A. BACKGROUND

Glenn Johnston, Ph.D ("Johnston") graduated magna cum laude with a Bachelor of Science degree in Physics from Carleton College in 1977, and in 1983 received a Master's degree and a Ph.D. from the University of Colorado. From 1983 to October 2007, Johnston worked for Los Alamos National Laboratory ("Los Alamos"), affiliated with the Department of Energy.

While at Los Alamos, Johnston obtained top-secret security clearance, formed a Vulnerability Assessment Team, published articles in peer review journals, and from 1992 to 2007, initially as a

technical staff member and later a team leader and section leader, worked hands-on with hundreds of different types of seals.

Currently, Johnston is employed at Argonne National Laboratory, also affiliated with the Department of Energy, as a Senior Systems Engineer and section manager for the Vulnerability Assessment team. The team examines a broad range of security devices, systems, and programs to identify security flaws and then suggests countermeasures.

Johnston is the author of over 115 publications in the areas of computer security, security culture, and tamper-indicating seals. Johnston often gives lectures regarding the interplay between cyber security and physical security, including: (1) two keynote addresses at cyber security conferences in Chicago and San Francisco; (2) a speech at an international security conference in Bahrain; (3) a presentation on "How to Conduct an Adversarial Vulnerability Assessment" at IMPACT 2006, a cyber security conference essentially run by the Department of Defense; (4) a presentation entitled "Security Vulnerability Assessments" at the Western OPSEC Conference; and (5) a live Internet presentation broadcast to eight different countries.

In addition to speaking engagements, Johnston has published approximately thirty articles specifically on security seals and detection, half of which have appeared in peer reviewed journals. He has also received numerous awards and acknowledgements: (1) a Distinguished Performance Award from the Central Intelligence Agency, the Los Alamos Lab in 2002; (2) an award in the sum of $3,000 for a Los Alamos Fellows prize for outstanding research in 2004; (3) two Los Alamos Distinguished Performance Awards in 1996 and 2001; (4) three Los Alamos Achievement Awards; (5) a $1,000 award for "Excellence in Performance Measure" from the American Society for Industrial Security; and (6) two National R&D 100 Awards.

Johnston has testified as an expert witness in three prior litigated matters. In the case before this court, he is serving without compensation. While he testified to having considerable experience and

knowledge of computer and cyber security, he also stated, "I don't think I would label myself first and foremost as a security - - as a computer security expert." [68] Tr. 1, 38:9-11.

Johnston is a Certified Protection Professional ("C.P.P."), with a certification from ASIS International, the Professional Association of Security Professionals. To qualify as a C.P.P., a candidate must possess a minimum number of years of experience in the security field and pass a comprehensive examination. The certification, renewed every few years, requires each candidate to demonstrate professional growth in the field of security.

In 2006, Johnston authored a paper in American Scientist, entitled "Tamper-Indicating Seals." His research regarding seals also appears in "New Research on Tamper-Indicating Seals" and "Nuclear Safeguards and Security: We Can Do Better," by Johnston, Warner and Garcia. Through these publications, Johnston examined 244 different seals. Approximately nineteen percent of the seals are in use somewhere in the world for nuclear safeguards, and fifty percent are in use for some kind of high level security application. Many of these are similar to padlock seals, pressure sensitive adhesive label seals and plastic strap seals.

The court qualified Johnston as an expert in physical security, security culture, and security methods, with an emphasis on security seals. Johnston authored two expert reports, one dated February 22, 2009 and a supplemental report dated April 19, 2009. The initial report addressed New Jersey's security culture and seals proposed by the State. The supplemental report addressed new seals and gluing processes proposed by the State after Johnston's examination of the AVC on April 16 and 17, 2009.

In the report, different terms are used to describe a piece of hardware or method for recording unauthorized access or tampering that has taken place. "A tamper-indicating seal" (often referred to as a seal) is also called a tamper-indicating device ("TID"). Unlike a lock, a seal does not resist unauthorized entry (except perhaps in some vague psychological sense). Expert Report, p. 4, ¶ 18.

[68] The four days of testimony are identified as follows: Tr. 1 (4/21/09); Tr. 2 (4/22/09); Tr. 3 (4/23/09); and Tr. 4 (4/24/09).

The sections that follow include information and recommendations offered in Johnston's expert reports and four days of trial testimony.

B. SECURITY CULTURE AND COGNITIVE DISSONANCE

According to Johnston, a reliable security program must have a carefully conceived and organized security culture. He defines security culture as a collection of formal and informal aspects of security. Formal aspects include such as rules, regulations, policies, and procedures. Just as important, however, are the informal aspects, such as attitudes towards security, the desire to have pro-active approaches to security, the ability to avoid cognitive dissonance, the tendency to not want to hear about security problems and other aspects associated with truly incorporating concepts of security, coupled with emphasizing that throughout the entire organization continually.

Johnston testified about a phenomenon in the area of physical security, known as convergence. Convergence occurs because physical security devices and systems increasingly have microprocessor firmware and computer software. Conversely, computer security and cyber security require an increased emphasis on physical security. As a result, professionals in security must consider that almost everything has cyber and physical security elements; to wit, a physical piece of hardware and a mechanism where there is something communicated either through a physical transmission line or through a wireless system.

During direct examination, Johnston identified a concept called cognitive dissonance. Identified by psychologists, this occurs when the majority of people want good security, yet evidence of security vulnerabilities creates mental tension. This results in individuals who are unwilling to consider potential problems or to pro-actively seek them out. Johnston described Giles and several of the lay witnesses in this case as exhibiting signs of cognitive dissonance by believing that, if an attack fails, the possibility of a viable attack is eliminated.

According to Johnston, the key element to understanding how someone might defeat a security device system or program is to view the program from the standpoint of a "bad guy." The key to this approach is to recognize the vulnerabilities that are most likely to be exploited or the easiest to exploit,

particularly since vulnerabilities are unlimited. Because it is impossible for a vulnerability assessor to demonstrate perfected attacks on all potential vulnerabilities, due to the lack of time, money, or resources, the preferred approach is to limit focus on the vulnerabilities that seem highly plausible and easy to exploit.

Over the years, the Vulnerability Assessment team has developed a great deal of expertise in identifying the vulnerability of seals and the means to perfect attacks. According to Johnston, a good security culture requires the organization to be pro-active with respect to security policies. This includes regularly examining internal weaknesses, anticipating attacks, and adopting a policy that security should remain an ongoing process.

To prepare for trial, Johnston reviewed the depositions of Giles, Gentile, Mahoney, and Clayton. Johnson concluded, from this review of witnesses, that: (1) there is "a rather alarming lack of a healthy security culture"; (2) there is no plan, strategy, or uniform policy for securing the voting machines either during storage, when transporting them, when locking them up, and when leaving them in different voting locations prior to the election; (3) the State relies on seal manufacturers and does not consult with independent security experts; (4) there is no seal-use protocol; and (5) the State does not conduct criminal background checks for employees, vendors, or consultants. Tr. 1, 58:20-21

As part of preparing for trial, Johnston did not interview any election officials or representatives, review any peer reviewed articles regarding New Jersey's voting machine security or conduct any research on the security culture as it relates to elections. Nor did he have any familiarity with Federal or State standards or regulations dealing with voting systems, or have any evidence of any incident of tampering of any voting machine in New Jersey.

When asked by the State whether it was possible to eliminate all security vulnerabilities in a system, Johnston responded:

> I do not believe that's possible.
>
> QUESTION: Would you agree that there is no way to guarantee absolute security in a voting machine?

> WITNESS: Yes. I believe, your Honor, any device or security device cannot be guaranteed with absolute security.
>
> QUESTION: Do you also believe that absolute security is a myth in any security application?
>
> WITNESS: Yes, I do.
>
> [Tr. 3, 79:11-80:2.]

Johnston also rejected a "perfection" standard for analyzing security. He noted, "I believe perfection is an inappropriate standard for any human endeavor, including analyzing security or executing security." Tr. 3, 80:5-8.

C. SEAL PROTOCOLS IN NEW JERSEY

According to Johnston, critical to any security plan is the development of seal protocols that detail exactly how a seal is used. Johnston defined a seal-use protocol as:

> [a] large collection of aspects of how the seal is used. It covers the cradle to grave span of the seal, everything from how one does choose the seal, procurement, storing the seal, transporting it, installing it, how it's inspected, how it's removed, how it's disposed of, how the training is accomplished, what types of personnel are going to be doing the inspections and the installations. A seal is essentially no better than its use protocol.
>
> [Tr. 1, 80:22-81:7.]

To defeat a seal, one has to remove the seal and then either reinstall the same seal or reinstall a counterfeit seal. In doing so, the person must perform in a manner that is not detected by the seal-use protocol.

D. SEALS AND IN-COURT DEMONSTRATION

In the early 1990s, Johnston studied a range of seals including government, commercial, passive, non-electronic, and electronic. These seals ranged from low-tech to high-tech. According to Johnston, the average time required to attack each of the seals was two to three minutes. The seals included: (1) padlock seals with similar concepts, but a different design than the Brooks padlock seal; and (2) different types of tamper-indicating tapes, with concepts similar to the current Brooks tape.

As part of the pending litigation, Johnston evaluated thirteen seals. The number of seals is large, in part, because the State changed a number of seals in response to expert reports associated with the

current litigation. Johnston criticized the State's quick turnover process for implementing seals inasmuch as: (1) introducing a new seal is a complex process that requires a completely different set of use protocols; (2) it takes several months to analyze the issues associated with the introduction of a new seal; and (3) swapping one seal for another without serious analysis shows a lack of understanding of the realties of tamper detection.

Johnston's report outlines the type of seal, the method of attack, and the time to defeat each seal. He testified that most seal manufacturers provide free samples. Currently, the State intends to use six seals in nine locations. One seal, the Brooks padlock seal, is a device with a blue interior body that looks like a padlock; it has a shackle and is locked closed. It is a tamper-indicating seal. There is an interior serial number and barcode that provides a unique fingerprint. Johnston testified that a laser printer and some image processing is all one would need to produce a counterfeit seal and barcode.

Johnston also examined the Brooks red adhesive label seal, two versions of the MRS2 adhesive label seal, a metal cup seal made by American Casting and Manufacturing, and a plastic strap seal made by Brooks. He described the MRS2 seals as: (1) sticky labels that, with careful handling, can be removed with solvents; and (2) low-tech attacks that require tools, materials and supplies that are widely available at a low cost. Anticipating that the State may add an ultraviolet mark, possibly a logo to the seal, Johnston testified that with inexpensive tools and supplies, available on the Internet, this is no different than counterfeiting a visible ink mark or logo.

Johnston also spent ten hours examining ways to defeat the Brooks red adhesive label seal proposed by the State. While the seal has a remarkably good adhesive, it is very difficult to apply the seal without damaging it, and Johnston noted that the serial number stays behind when the seal is removed. According to Johnston, when every single tape removed has visible damage, the inspection of the seal is compromised. Johnston devised an attack and demonstrated it in court.

Johnston evaluated several different versions of plastic strap seals. The most recent recommended by the State is a Brooks blue plastic strap type 2 seal. With proper training and understanding of likely attack scenarios, these types of seals are more reliable than pressure-sensitive adhesive label seals and

provide some possibility of detecting tampering. Without training, they are not reliable. By creating a device, built from part of a coke can, it took Johnston three seconds to defeat the seal. He described this as a widely known technique.

Johnston also evaluated two sizes of cup seals made by American Casting and Manufacturing: (1) the MCS-C (half-inch smaller size);[69] and (2) a larger size. According to Johnston the smaller size will no longer be available and for the limited stock available, there will no longer be the imprinting of serial numbers.[70] Johnston testified: (1) the attacker can use a battery powered hand drill which Johnston's colleagues used to defeat the seals in three to ten minutes; (2) there is no security without a serial number; (3) the seal does not represent reliable tamper protection; (4) a hobbyist can create a counterfeit logo or serial number on the top half of the seal; (5) it would take a sophisticated use protocol to detect this attack; (6) the proposed location of the seals make inspection difficult; and (7) the use of Gorilla glue in the cup seals renders the use highly problematic.

The amount of time Johnson spent to evaluate each seal varied: (1) the Brooks padlock seal took approximately twenty hours; (2) the American Casting & Manufacturing MSC-C cup seal took approximately three hours with the unglued cup-seal and ten hours with the glued cup-seal; (3) the plastic Brooks blue strap seal took approximately one hour; and (4) the additional plastic strap seals each took ten minutes each. The State has elected not to use the larger cup seal.

While the court does not impute any ill intent on his part, the record disclosed that Johnston commingled many of the damaged seals with his personal collection of seals, located at his home or at the laboratory at Argonne. These seals originated from other vendors, and relate to pending and past seal cases submitted by the government and private individuals or companies. As a result, during the trial, Johnston was unable to differentiate many of the seals provided by the State from seals from other

[69] The State plans to insert Gorilla brand glue into the seal.

[70] Giles testified that American Casting and Manufacturing, through a special order with the State, plans to provide a cup seal with a serial number. This agreement has not been reduced to writing.

sources. Nor was he in a position to testify as to the exact number of seals examined from the State, or the percentage that were damaged.

At several points during cross-examination, Johnston acknowledged intermingling seals. He responded affirmatively to the question, "did you intermingle the seals that you received from counsel or Professor Appel with the ones that you received directly from Brooks or the other vendors"? Tr. 3, 11:18-22. Later in the day, referring to multiple projects, Johnston noted:

> Well, your Honor, as is typical the situation when we have multiple projects involving seals, we tend to combine studies and combine samples thus the natural tendency for me to take various seal samples and combine them into a single source. Some of the research we were doing on seals was for purposes of understanding potential seal usage on the Advantage voting machine for the benefit of the Verified Voting Foundation.
>
> [Tr. 3, 111:9-17.]

Johnston acknowledged using New Jersey seals and other seals for projects totally unrelated to the pending litigation. Johnston noted that instead of using voting machines to practice defeat seals, "we just practiced with them as independent seals not connected to anything." Tr. 3, 136:14-15.

Johnston acknowledged experimenting with seals at plaintiff's home and Appel's home on April 15 and April 16, 2009:

COURT: And the Saturday and Sunday, you experimented also?

WITNESS: Yes.

COURT: And where were you?

WITNESS: At plaintiff's home and at Professor Appel's home.

COURT: Do you recall how many you experimented with?

WITNESS: No.
COURT: Approximately?

WITNESS: I would estimate 25.

COURT: Were any of them damaged?

WITNESS: Yes.

COURT: Approximately how many?

WITNESS: Most of the 25, or all.

COURT: All right. Did you try to defeat any?

WITNESS: Yes, I believe some of the tests I was running involved attempted defeat.

COURT: And were any of them damaged in the process?

WITNESS: Yes.

COURT: Do you know how many?

WITNESS: Most of them, I was exploring alternative attacks.

COURT: So, the result was different than what I saw in the courtroom?

WITNESS: Yes.

[Tr. 3, 56:20-57:25.]

E. IN-COURT DEMONSTRATION

The supplemental report, dated April 19, 2009, includes an examination of the six seals contemplated by the State for use in nine locations in the next election. This examination was conducted at the Justice Complex on April 16 and 17, 2009.

At trial, Johnston demonstrated each of the seals now proposed for use in the voting machines. These seals include: (1) the Brooks padlock seal with a serial number;[71] (2) the Brooks red pressure sensitive adhesive label seal;[72] (3) two versions of the MRS2 adhesive pressure sensitive adhesive label seals;[73] (4) the American Casting and Manufacturing MSC-C metal cup seal; (5) the Brooks gray MRS seal; and (6) the Brooks plastic strap seal.

With regard to each of the six seals, Johnston testified that there are major problems related to

[71] The State plans to use Gorilla brand glue inside the padlock seal.

[72] The Brooks Red Pressure Sensitive Adhesive Label Seal has a serial number on the right lower corner. According to Johnston, modified seals can be prepared in advance by removing the adhesive and serial number from underneath the semi-transparent red window at the low right corner of each seal.

[73] The State intends to add an ultraviolet logo to the MRS seals.

installation, removal, and the ability to identify tampering. First, the American Casting & Manufacturing MSC-C cup seal will need to be removed periodically for three reasons: (1) to replace the battery; (2) to inspect the internal electronics and seals on the ROM chips; and (3) to look for evidence of tampering. If glue is used in the metal cup seals, this will make removal of the cup seals and inspecting their interior for evidence of tampering more complicated.

As to the Brooks red pressure sensitive adhesive label seal, this seal is extremely sticky and difficult to apply without damage. This makes installation difficult, unpleasant, and time-consuming. Most significantly, it also makes it very difficult for seal inspectors to distinguish between inadvertent damage occurring at the time of seal installation and potential attack attempts.

The plastic strap seals can be removed using simple tools, and reused leaving no visual evidence that they have been opened. This takes less than thirty seconds. The State of New Jersey proposes to use Gorilla brand glue inside the padlock seal. According to Johnston, the insertion of glue will not improve tamper detection. Since the glue flows in unpredictable ways, through and around the bar-coded label, every seal will be different. This unpredictable pattern makes it much more difficult to train seal inspectors for evidence of tampering.

Finally, the State intends to add an ultraviolet logo to the MRS seals. Johnston did not know the nature of the logo. He testified, however, that UV inks and illuminators are readily available to the general public, and a rubber stamp can be made of almost any design by many companies. This design can be easily imprinted on paper.

Before the in-court demonstration began, Johnston assembled all of the tools required to remove and re-install the seals. Assembling the tools took approximately ten minutes. The in-court demonstration of the six seals contemplated for use in New Jersey lasted two hours, sixteen minutes, and sixteen seconds.[74] Johnston began the court demonstration to defeat the tamper evident seals on April 23, 2009, taking one hour, eleven minutes and twenty-three seconds. The second day, April 24, 2009, Johnston

[74] A timing device, placed on the judge's bench, measured the time from start to finish. This time did not include the ten minutes to assemble the tools, as noted above.

continued the demonstration with a time of one hour, four minutes, and fifty-three seconds. Johnston prepared all the counterfeit seals in advance of the court demonstration. It took an additional one minute and fifty-seven seconds to clean the area surrounding the voting machine. This is the period of time it would take an attacker to open the machine, remove any necessary internal parts, defeat the seals, replace the seals, and close the machine.

Johnston testified that the materials to defeat the seals are readily available in retail stores or on the Internet. These include simple tools such as bolt cutters, a battery-operated hand drill, a hot air gun, hot glue gun, screwdrivers, wrenches, a tool bit kit, and pliers. The solvents to remove seals include acetone, commonly found in nail polish remover. Lastly, a small printer may be used to create counterfeit serial numbers or graphics.

After the demonstration, Johnston reviewed each of the seals to determine whether the seals had been defeated. In making this assessment, Johnston applied the following: (1) a no seal-use protocol, with no training; (2) a seal-use protocol, with modest training; and (3) a seal-use protocol, with a high level of training. Based on Johnston's testimony and results of the demonstration, the court finds that the likelihood of detecting tampering increases as one moves from a no seal-use protocol to a high level seal-use protocol.

In his report, Johnston states:

> I can state to a reasonable degree of certainty that the seals and security measures proposed by New Jersey to provide security for the AVC Advantage voting machines are insufficient to guarantee election integrity. The skills, time and resources to spoof these seals and security measures are not a major barrier to an adversary, and are, in fact, widely available.
>
> [Expert Report, ¶ 154, p. 34.]

Johnston testified that "poor security practices involved in the storage, transport and chain of custody for the voting machines are troubling as well." Expert Report, ¶ 156, p. 34. Furthermore, even if the State adopts seal-use protocols, substantial time and costs would be required to inspect the different types of seals.

New Jersey is proposing to add six different kinds of seals in nine different locations to the voting machines. Johnston testified he has never witnessed this many seals applied to a system. At most, Johnston has seen three seals applied to high-level security applications such as nuclear safeguards. According to Johnston, there is recognition among security professionals that the effective use of a seal requires an extensive use protocol. Thus, it becomes impractical to have a large number of seals installed and inspected. He testified that the use of a large number of seals substantially decreases security, because attention cannot be focused for a very long time on any one of the seals, and it requires a great deal more complexity for these seal-use protocols and for training.

F. TIME AND COST FOR EFFECTIVE SEAL PROTOCOLS

While Johnston testified the actual attacks require limited skill, to train a seal inspector requires in excess of twelve hours per seal. As noted by Johnston in his report:

> [u]nlike defeating other kinds of security devices, defeating seals is primarily about fooling the seal inspector. Any evidence of seal tampering left after the attack is irrelevant if the inspector doesn't see it, isn't psychologically prepared to see it, or doesn't want to see it. I have studied a number of tamper detection programs where the seal inspectors do not want to report suspicious seals because of the consternation this causes their supervisor.
>
> [Expert Report, ¶ 57, p. 10.]

Without the latest proposed seals from the State, Johnston estimated the cost and time as 298 days plus 92 days for the inspection of the 11,000 voting machines in New Jersey. This results in up to fifteen minutes per voting machine, per election, resulting in 344 additional days of labor. The cost per election to effectively inspect and install the seals is $492,000, due to the highly complex proposed configuration. Furthermore, a good seal-use protocol takes one to three months to develop, per seal. Based on this estimate, according to Johnston, it would take approximately eighteen months for New Jersey to develop an effective seal-use protocol. The cost to develop an effective security protocol may be in the range of $50,000 to $300,000 per seal.

Johnson described the seals applied to the AVC as a band-aid approach to deal with the security vulnerabilities inherent in the voting machine.

G. REVIEW OF THE DEPOSITION OF STATE'S WITNESSES

After reviewing the depositions of Giles, Gentile, Mahoney, and Clayton, Johnston concluded New Jersey has an unhealthy security culture. Further, a seal manufacturer with a monetary interest in selling products is not the appropriate party to consult with in selecting a particular seal. Instead, the State should consult with outside independent security professionals. Johnston did not find any evidence, in any of the depositions, of efforts by the State to solicit advice from independent internal or external security experts.

In response to Giles' testimony that physical security requires a kind of band-aid approach, where serious vulnerabilities can be covered over with ad hoc fixes or the equivalent of software patches, Johnston stated, "nothing could be further from the truth." Expert Report, ¶ 64, p. 12.

Moreover, Johnston stated that Clayton's testimony described a poor chain of custody in regard to transportation and storage, specifically: (1) there is a poor chain of custody as to the transportation, arrival, and storage of the voting machines at the warehouse; (2) there are no written policies for storage and security; (3) the record reflects there is no video-monitoring of the voting machines at the polling places; and (4) voting machines are not placed in secure locations, before or after elections, at the polling site. Expert Report, p. 15.

The problems with the transportation and storage of the voting machines surfaced in the deposition and trial testimony of Mahoney and Gentile. In both counties, Mahoney and Gentile testified that voting machines are left out in public areas for up to two weeks with little or no protection. Both Mahoney and Gentile did not know whether the vendors providing for the transportation of the voting machines were required to undergo criminal background checks.

H. CONCLUSION

Johnston concluded that:

> The tamper-indicating seals, their use protocols and other security measures proposed by the State are not sufficient to detect or deter tampering with the AVC voting machine. The adversary needs to be motivated, willing to practice the attack, and moderately resourceful. He

> does not, however, need high technology, or rare/expensive skills, tools, techniques or materials to surreptitiously tamper with voting machines.
>
> [Expert Report, p. 3, ¶ 12.]

Regarding the State's intent to use six different kinds of seals in a total of nine different locations, Johnston testified, "in 17 years of seals experience, I have never encountered a security application that used more than three tamper-indicating seals on any container, including for nuclear security applications." Report, ¶ 2, p. 33

16. WAYNE HENDRIX WOLF (EXPERT FOR PLAINTIFF)

A. BACKGROUND

Professor Wayne Hendrix Wolf ("Wolf") received a Bachelor of Science degree in Electrical Engineering from Stanford University in 1980, a Master of Science degree from Stanford University in Electrical Engineering in 1981, and a Ph.D. from Stanford University in Electrical Engineering in 1984. Currently a professor at the Georgia Institute of Technology ("Georgia Tech"), Wolf holds the formal title of Rhesa Ray S. Farmer, Jr., Distinguished Chair of Embedded Computing Systems and Georgia Research Alliance Eminent Scholar. From 1989 to 2007, Wolf served on the faculty of Princeton University.

Wolf has taught many courses related to the study of microprocessors, including: (1) embedded computing courses; (2) an introductory course at Georgia Tech; (3) a course developed at Princeton University in computer structures that provides students the opportunity to design the logic and implement a FPGA; (4) a course at Princeton University in very large scale integration ("VLSI"), that is, the design of integrated circuits and laboratories where students design simple microprocessors; (5) a course at Princeton in computer systems that includes microprocessors and computer architecture; and (6) courses at Princeton University and Georgia Tech on embedded computing that use microprocessors for real-time applications ranging from digital still cameras to automobiles.

Wolf has served as Editor-in-Chief of the Association for Computing Machinery ("ACM") in embedded computing systems and IEEE Transactions on VLSI systems, and is the author of four major

textbooks dealing with different aspects of microprocessors, including: (1) VLSI; (2) FPGA-based system design; (3) an undergraduate textbook on embedded computing; and (4) a graduate textbook on embedded computing.

In addition, Wolf is the author or co-author of over 200 technical publications, including a great deal of work published over the past twenty-five years on microprocessors, embedded software, logic design, and FGPA-based system design. Wolf is also the named inventor on eight United States patents and has served as a consultant and as a member of the Board of Directors to several companies. Wolf has testified as an expert witness in several patent lawsuits in the Federal District courts involving FPGA-based emulators, train airbrake design, and smart cameras. Wolf is familiar with several techniques to identify fraudulent chips: (1) watermarking digital design; (2) x-ray techniques for examining chips; (3) delidding; and (4) measuring radio frequency emissions from chips. The court qualified Wolf as an expert witness in the areas of microprocessors, embedded computing, logic design (including FPGAs), VLSI design, and embedded system security.

Wolf, who is serving in this matter pro bono, addressed two issues: (1) the feasibility of creating a fake Z80, a modified microprocessor that can be used to change election-related data on a voting machine; and (2) the countermeasures proposed by the State to detect the fake Z80 and its associated hardware.

The sections that follow include information and recommendations offered by Wolf, by video, during trial and as set forth in his expert report.[75]

B. THE Z80 MICROPROCEESOR

The Z80 is a microprocessor architecture that has been embedded in a number of different chips. Since the technology was introduced over thirty years ago, the Z80 chip is not considered state-of-the-art today. Portions of Wolf's Expert Report respond to the reports of various experts put forth by defendants and, more specifically, Sequoia's October 2, 2008 rebuttal report. On page five, paragraph seven of Wolf's expert report, Wolf challenges the notion by Smith that the prospect of creating a fake Z80 is a fantasy.

[75] Wolf testified by video on May 11, 2009.

According to Wolf:

> There are logic designs for real Z80s available for free on the Internet – or at least widely available on the Internet without an upfront charge. And modifying that in order to execute one's own software is very straightforward, and implementing that in a couple different ways is very well known and straightforward.
>
> [Tr. 30:10-17 and Expert Report, p. 5, § 7.]

Furthermore, Wolf testified that the logic design could be achieved by a college junior, in the appropriate study program, and VLSI could be completed by either a college senior or Master's degree student.

C. A FRAUDULENT Z80 CHIP CAN MASQUERADE AS A Z80

Wolf disputed claims by the defense that no one has demonstrated that a fraudulent Z80 chip could successfully masquerade as a Z80 or that it is useless to worry about a fake Z80. Wolf described two ways in which a fake Z80 could masquerade as a real Z80. According to Wolf, it is possible: (1) to place the chip for the fake Z80 in the real Z80's package; (2) to make the chip inside the package resemble the physical characteristics of a real Z80, such as making certain that the chip is the right size and shape, or by adding metal layers on top of the chip to look like the wires on the real Z80; (3) to secure the logic design for a Z80 on the Internet; (4) that a VLSI fraudulent Z80 could fit the additional logic and memory required to trick a voting machine; and (5) to build a VLSI fake Z80, which is a semi-custom or custom-integrated circuit.

Regarding the creation of both a FPGA fake Z80 and a VLSI fake Z80, Wolf estimates that approximately 10,000 practitioners in the United States possess the requisite logic design skills to create a Z80 to manipulate a voting machine. Furthermore, some of Wolf's earlier articles quote a source stating that at least half a million practitioners around the world have embedded computing software skills.

In response to a question as to the length of time required to create a fake Z80, Wolf responded:

> (1) The logic design for the fake Z80, which executes malevolent software, takes approximately 56 hours to create, including creating an FPGA implementation.[76]
> [Tr. 32:20-25.]

[76] According to Wolf, one of his former students would be able to create a fake Z80 in this amount of time.

> (2) If one wanted to create a VLSI implementation, a semi-custom or custom chip, I estimated about a thousand hours which is roughly six months.
>
> [Tr. 33:2-5.]
>
> (3) The logic design could be done by a college junior in the appropriate study program and VLSI design could be completed by a college senior or master program student.
> [Tr. 33:13-16.]
>
> (4) Well, once you have the logic design for the fake Z80, you would use computer-aided design tools to unmap that design into the FPGA. Some versions of these tools are actually available free from Xilinx, for example. You can also use tools at what I consider to be a pretty nominal cost, a few thousand dollars.
>
> [Tr. 35:2-7.]
>
> I found a quote for a Xilinx FPGA of $15.84 and that's for a quantity of one. I believe you could get a cheaper price if you ordered a large number of them.
>
> [Tr. 34:22-24.]

D. WOLF'S RESPONSE TO STATEMENTS BY TERWILLIGER

Wolf challenged four statements by Terwilliger that address a broad range of issues, including whether a FPGA has sufficient memory to hold the software required to control the program needed for a fake Z80. The words before "whereas" represent the purported incorrect statements by Terwilliger followed by the corrected language inserted by Wolf:

> A semiconductor memory is implemented in logic gates, whereas it is in fact implemented with specialized circuits.
>
> The basic unit of capacity for an FPGA is a "gate," whereas Xilinx FPGAs use static CMOS configuration latches to implement their logic gates. That SRAM can also be used directly as memory.
>
> Most FPGAs have a limited amount of memory, whereas many FPGAs have large amounts of on-chip memory.
>
> An attacker would have to store both unmodified and modified software in the FPGA, whereas not all of the voting machine memory contents would have to be resident on the chip.
>
> [Expert Report, p. 8.]

During direct examination, Wolf reviewed the steps required to implement the fake Z80 microprocessor after it is manufactured. In order to facilitate effective use, the chip must be placed in a package. The FPGA package is distinguishable from the Z80 package. Thus, in order to better disguise the FPGA, it is possible to place it in a package similar to the Z80 package, with the appropriate manufacturing markings, so that it looks like it came from Zilog or another manufacturer.

Wolf explained the Dual Inline Package ("DIP"), rectangular in shape with pins along two sides that allow for electrical connections. In terms of the cost of repackaging a fraudulent chip, that depends upon the packaging material. Plastic packages are less expensive at approximately $8 per unit. Ceramic packages are more expensive at approximately $55 per unit.

E. COUNTERMEASURES BY SMITH AND TERWILLIGER

To summarize, Wolf evaluated the countermeasures proposed by Smith and Terwilliger, and found:

> (1) with respect to the visual inspection of a chip after delidding, as seen in photographs in Smith and Terwilliger's expert report depicting the difference between a Z80 microprocessor and an FPGA microprocessor it is possible to repackage the Xilinx FPGAs to look like the Zilog Z80;
>
> (2) an x-ray analysis is not necessarily an effective technique for detecting a fraudulent Z80 chip;
>
> (3) it is possible for x-ray analysis to damage the underlying computer;
>
> (4) delidding is an insufficient method for detecting a fraudulent Z80 using the VLSI technique;
>
> (5) the motherboard may be damaged by implementing the delidding technique, and it definitely renders the chip unusable;
>
> (6) in order to implement the delidding technique, the chip must be removed;
>
> (7) once the chip is removed, it is sent to a delidding facility where it is delidded and compared with a known good chip;
>
> (8) radio frequency analysis is not an effective means of detecting a fraudulent chip;
>
> (9) assuming that an individual reaches the radio frequency using a

reliable and effective method, which may require various degrees of disassembly of the voting machine, the frequencies must be deciphered using the necessary signatures;

(10) it is possible to design a fake Z80 that emits the radio frequency signature of a real Z80, in which case it is necessary to wait for the fake Z80 to perform some illicit operation before it is possible to identify fraud and, even then, there must be an existing signature to provide information that the fake Z80 is acting improperly; and

(11) it is erroneous to assume that all the Zilog parts used in the voting machines in New Jersey are the same, because in terms of the Zilog parts used in the voting machines in New Jersey, these parts affect the packaging, die size, visible circuits, and radio frequency emissions.

[Expert Report, pp. 20-26; Tr. 43:14-52:11.]

F. CREATING A FAKE Z80 TO MANIPULATE ELECTION RESULTS

During cross-examination, Wolf conceded the following points: (1) the time required to make a FPGA simulate a Z80 would take about 56 hours, and the cost for 500 units is $70 per unit, thus amounting to $35,000; (2) the same cost of $70 applies to 10,000 units, thus amounting to $700,000; (3) the time required to make a VLSI simulate a Z80 would take about 1,000 hours, and cost for 500 units is $640 per unit, which amounts to approximately $320,000; and (4) if 10,000 units are purchased, the cost is $80 which amounts to $800,000. According to Wolf, the costs include both the silicon and the packaging, but he is unclear of whether the packaging is ceramic. With respect to the FPGA, Wolf did not include the cost of time required to actually design the logic, which may potentially increase the cost.

Responding to questions regarding the counter-measures proposed by Smith and Terwilliger, Wolf acknowledged that he had never created a fake Z80 to:

(1) manipulate election results on a AVC;

[Tr. 56:19-22.]

(2) manipulate election results on an AVC Advantage and embodied in FPGA;

[Tr. 57:9-14.]

(3) manipulate election results embodied in a VSLI chip;

[Tr. 57:5-8.]

(4) manipulate election results on an AVC, embodied it in either an FPGA or a VLSI chip, and installed it into a voting machine and had it work;

[Tr. 57:9-14.]

(5) manipulate election results on an AVC, embodied it in an FPGA, installed it in the machine and then used the visual inspection technique discussed in the expert reports to determine if the fake Z80 could be detected;

[Tr. 57:15-22.]

(6) manipulate election results on an AVC and embodied it in an FPGA or VLSI chip and use the x-ray technique, delidding technique, or radio frequency analysis to determine whether or not he could detect the fraudulent Z80;
[Tr. 57:24-58.4.]

(7) manipulate election results on an AVC voting machine, embody it in a FPGA and use the delidding technique to determine whether or not he could detect the fake Z80;

[Tr. 58:5-9.]

(8) manipulate election results on an AVC voting machine, embody it in a FPGA and use the radio frequency technique to determine whether or not he could detect the fake Z80;

[Tr. 58:10-15.]

G. CONCLUSION

In describing the creation of a fake Z80 and the related cost, Wolf noted that:

> [a] series of technical advances have made the design and manufacturing of fake Z80s well within the means of attackers. When I was an undergraduate at Stanford, the Z80 was a state-of-the-art chip. Today, it is well-understood and easily replaced technology. The logic design of a fake Z80 would start from Z80 designs available over the Internet and could be completed in less than two weeks time. Inexpensive FPGAs could be used to embody the fake Z80 and these fake Z80 FPGAs could be packaged to evade visual inspection of the motherboard. An attacker could build a VLSI fake Z80 with a fake top layer that would evade visual checking of the chip even after delidding.
>
> [Expert Report, pp. 26-27.]

Finally, as for the feasibility of checking for fake Z80s, Wolf emphasized that the "methods for checking for fake Z80s are not feasible or cost-effective. They require significant manipulation of the machine, which costs time and money. These manipulations also risk breaking the voting machines." Expert Report, p. 27.

IV.

ANALYSIS

A.

VOTING PROCEDURES IN NEW JERSEY

In eighteen of the twenty-one counties, voters in this State cast their vote on AVC Version 9.00H.[77] All twenty-one counties use electronic voting machines.

The AVC is a paperless full-face DRE in which voters select candidates through a user interface to a computer. The full-face machine permits the voter to view the contents and candidates' names at one time. The face of the official ballot is identical to the sample ballot received by the voter. The voter panel consists of a 38 x 28 inch panel with 42 rows and 12 columns of buttons, each with a green X-shaped LED light next to it. Covering the panel is a large sheet of paper with a printed facsimile of a ballot that lists contests, candidates, and ballot questions, corresponding to the buttons on the panel.

The panel contains a two-dimensional array of buttons and lights. Markings on the paper are placed over the buttons that are pressed for the corresponding candidates. When the LED lights up, it shines through the paper and is visible to the voter. To select a candidate, the voter presses the square button to the right of the name and the green "X" light will appear to indicate the voter's selection. The voter can change the selection by pressing the same box a second time and the "X" light will disappear. The write-in keyboard, located below the voter panel and to the left, has an LCD display. To the right is the "cast vote" button.

[77] In three counties citizens vote on: Sussex (401 iVotronic, ES&S); Warren (200 Avante touch screen EVC308FF); and Salem (160 Sequoia Pacific EDGE).

The procedures from county to county are quite similar. Prior to the election, the Clerk in each county prepares the ballot definition. The ballot definition includes the names of the candidates, the names of the contests and identifies the buttons on the AVC that correspond to each candidate. Once completed, the ballot, as wide as the front panel of the voting machine, is sent to the printer to produce as many copies as there are voting machines. By statute, a sample ballot is sent to each registered voter prior to the election. N.J.S.A. 19:14-21

When the ballot definition information is completed, it is copied to a results cartridge, the size of a VHS tape, using an ordinary laptop computer. Each laptop is equipped with WinEDS. As noted heretofore, WinEDS is a special software application that joins together the Microsoft operating system and an election data system software application, a Sequoia product. WinEDS is a special election data management system that runs on the Microsoft Windows operating system.

To achieve the transfer, the WinEDS enabled laptop computer is attached to a cartridge reader. The cartridge reader has a Universal Serial Bus ("USB") connector that plugs into the laptop. Using the WinEDS enabled computer, the information is copied onto the results cartridge. Once the transfer is complete and the information is downloaded onto the results cartridge, each results cartridge is placed in a slot-type metal cartridge receptacle located in the voting machine.

This transfer, also referred to as cartridge burning, generally takes place at the warehouse where the voting machines are stored. Once the cartridge is placed into the machine, the election worker turns on the machine. At that point, the menu on the operator panel instructs the computer in the machine to copy the data ballot information into the internal memory of the machine. After this occurs, the technician or consultant installs a seal through the hole in a metal cartridge receptacle to secure the cartridge in place. When the machine arrives at the polling location, the download has already occurred and the seal should be securely in place. The seal goes through holes in the metal cartridge receptacle and the cartridge itself.

Prior to an election, election staff prepares the voting machines for the election. This is conducted through the operator panel, by way of prompts that follow a sequence of commands to test the various components of the voting machine. During trial, fact and expert witnesses testified regarding the Pre-LAT

mode. In Pre-LAT, election officials, consultants, or third party vendors test the ballot definition to make sure the names are printed over the right buttons. The machine can be set in Pre-LAT or Official Election mode. After the ballot definition has been transferred to the internal memory, the machine is ready to run a Pre-LAT test.

Pre-LAT, in essence, is a mock election in which election staff or third party vendors/consultants cast votes for different candidates and then print the results to compare the totals. The internal printer, found in each machine, prints the number of votes cast for each candidate. Once the election worker turns the key switch to open the polls, the number should be zero, also referred to as a "zero" tape. Once casting votes for the mock election is completed, the election worker turns the key switch back to close the polls. At that point, a new printout is made and a comparison of the actual votes cast with the print out is achieved.

After Pre-LAT is completed, the machine is then ready to be transported to the polling place. Based on the testimony adduced at trial, the time between Pre-LAT and the transportation of the machines to the polling place varies from one week to more than a month.

The day of the election, poll workers arrive early with election materials and the keys to each machine. The poll worker turns the switch from "polls closed" to the open position, and the printer prints out how many votes have been recorded for each candidate. This should produce the "zero" tape. Each voter receives an authority slip to vote. At the end of the evening, the poll worker turns the switch to the closed position. At that point, the printer automatically begins to print a results report listing how many votes each candidate has received. In a primary election, the report will list how many voters were activated to vote in the Republican primary, and how many voters were activated to vote in the Democratic primary. The results report also contains the date and time, precinct number, machine serial number, protective counter, and public counter. The protective counter is how many votes have ever been cast on this machine, while the public counter is the number of votes cast in a particular election.

There is a space on the print out for the poll workers to sign to verify that this paper came from a particular machine. At that point, the poll workers are trained to remove the cartridge by cutting the seal

with scissors and recording the serial number of the seal on the results cartridge print out. During the trial, evidence was presented to establish that recording of the seals is not always done.

The results cartridges are transported to either satellite offices or a central location. The results cartridges are placed into a cartridge reader that is connected to the WinEDS enabled computer. The vote totals from the results cartridges are entered into the computer and produce a report similar to a spreadsheet. The report is then compared to the printout from the machines.

If the voting machine is equipped for audio voting, an audio-ballot cartridge containing ballot names and pronunciation goes in the daughterboard. If enabled, the voter wears headphones to listen to a voice mail menu. There is separate firmware that operates the audio voting.

In all of the counties, the voting machines are stored in a warehouse either owned or rented by the county. Three election representatives, responsible for the storage and transportation of voting machines, testified to similar procedures. Each of the buildings where voting machines are stored is equipped with an alarm system, and each election staff member has a unique code for access and a unique code for the alarm system. None of the sites are monitored by security cameras or assigned security personnel.

For the most part, keys for voting machines are maintained in locked cabinets, and duplicate sets are available if the original is lost. Furthermore, the laptops and results cartridges used by the warehouse are maintained in locked cabinets and storage areas.

Poll workers arrive early in the morning before the polls open to prepare the machines for voting. The voting machines are unfolded, the privacy curtains are installed, and the operator panels that hook onto the side of the machines are removed by the poll workers to perform two different kinds of functions. One is while the polls are open and the other is while the polls are closed. The operator panel has a liquid crystal display that can accommodate several lines of text.

After the machine is opened, the poll worker turns the power on-off switch to activate the machine. Separate from the on-off switch is the switch to designate polls open and closed. The switch on the back of the machine is in the closed position. Until five minutes before the polls open in the morning, the poll worker turns the switch to the open position and removes the key. Each voting machine is

equipped with a printer located on the back of the machine. The printer is activated and prints a report when the switch is turned to the "on" position. When the switch is turned to the "off" position, the machine again is activated to print a report. While the votes are being cast the printer is inactive.

Before a voter is permitted to vote, an election representative will verify the name and address of that registered voter. Once verification is completed, the voter then signs the poll book. Once completed, the poll worker gives the voter a "Voting Authority" slip that bears a serial number. The voter then hands the slip to the poll worker. If the election is a general election, the poll worker activates the DRE by simply hitting the green "activate" button. If it is a primary election, an insert fits into a slot on the operator panel. The insert has a Democratic label on one side and a Republican label on the other side. During a primary, there are two different buttons that are pressed. One is the Democrat or Republican button, either on the left or right. Once that is pushed, then the operator presses the green "activate" button.

On the other side of the machine, an "operator panel" contains additional buttons and an LCD alphanumeric display with two rows of 24 characters each. During an election, before each voter can vote, a poll worker must press a button on the operator panel to activate the machine to accept votes. The poll worker activates the button upon being handed a paper ticket by the voter.

At the close of the polls, the results are known in one of three ways. First, the AVC prints a paper print out of candidate totals. The printer is located on the back of the machine. Second, it writes these totals (along with a record of the votes cast in each ballot, the "ballot image") to a results cartridge, which is then removed from the voting machine. Third, it keeps these totals (with ballot images) in its internal memory. Election workers can extract this information from the AVC by using the menu buttons on the Operator Panel; the machine can be instructed to print the internally stored data onto its printer, or copy it to a fresh cartridge. The program in the computer stores data in its memory that should correspond to the actual number of votes. At the close of the polls, the computer outputs the number of votes for each candidate.

When the polls close, poll workers fold up the front of the machines, open the back doors of the machines, and use keys to switch the polls open/polls closed switches to the "closed position." As soon as the key is turned to the "polls closed" position, the printer automatically starts printing out a results report. The results report includes the date and time, precinct number, election district, machine serial number, protective counter (the number of votes cast on that machine in its lifetime) and the public counter (the number of votes cast in the election). After the printout, or while it is printing, the poll worker removes the cartridge that contains all of the information. The poll worker cuts the seal with a pair of scissors. Poll workers are directed to sign the paper print out and record the serial number of the seal from the results cartridge. To remove the results cartridge, the seal must be removed.

Following this, the results cartridges and seals are placed in a canvas bag and transported to a central location where the cartridges are tabulated. The voting machines are closed, locked and left at the polling places.

Unofficial election results are obtained within an hour or two after the election by means of the electronic tabulation of the cartridges. At the Municipal Clerk's office, a central location and/or one of several satellite offices, a computer reads the vote total from each results cartridge and enters the total for each election district into a database.

B.

SCOPE OF REVIEW

The extensive procedural history is set forth in the beginning of this opinion. Therefore, the court need not repeat it here. On June 29, 2006, the Appellate Court held:

> Therefore, every perceived constitutional deficiency in the electoral process would be remedied by a timely and successful implementation of the law. As a result, the issues presented to us on this appeal are mooted by the new legislation. We recognize, however, that the constitutional issues would remain if the legislation is not timely and successfully implemented, as the State and Attorney General have represented, in their brief and argument before us, it would be.
>
> [Gusciora, supra, 395 N.J. Super. at 426.]

As to the separation of power issue, the Appellate Division distinctly addressed this issue by noting:

> If there is a constitutional issue presented by the lack of implementation of the new law and an appropriate record can be made to support the constitutional claim of disenfranchisement, there would be no separation of power issue preventing the Law Division's consideration of the matter.
>
> [Id. at 427.]

In vacating the dismissal of plaintiffs' complaint and remanding the matter to the Law Division to conduct such case management conferences and hearings as necessary to monitor compliance with the new legislation, the Appellate Division distinctly set forth the parameters of the trial court's review:

> Should the legislation not be implemented as assured by the State and Attorney General, for development of a record with respect to the constitutional claims and for consideration of any appropriate remedy with respect thereto.
>
> [Ibid.]

The complaint, consisting of eighty-nine paragraphs, alleges the continued use of DREs violates: (1) the Constitutional requirement in N.J. Const. Art. II, § 1, ¶ 3(a) that every vote be counted; (2) the guarantee of Equal Protection in N.J. Const. Art. I, ¶ 1; (3) the statutory guidelines for recounts found in N.J.S.A. 19:28-1 et seq.; (4) the statutory requirement that each voter's intent be tabulated in accordance with N.J.S.A. 19:48-1(d) and (f), and N.J.S.A. 19:53A-3(b); (5) the statutory requirement that voting equipment be secure as mandated by N.J.S.A. 19:53A-3(g); and (6) the statutory requirement that votes be counted accurately, N.J.S.A. 19:48-1(h) and N.J.S.A. 19:53A-3(h).

While plaintiffs have not amended their complaint, plaintiffs apparently are no longer seeking judgment to require the State to retrofit all DREs with a VVPAT. Instead, plaintiffs now seek an order to decommission the AVC and to require the State to purchase precinct-based optical scan voting machines in all twenty-one counties.

Inasmuch as the constitutional and statutory claims are inextricably connected, the court rejects the notion by the State to dismiss the statutory claims

C.

FEDERAL AND STATE STATUTES AND REGULATIONS

During the pre-trial phase and trial, counsel for both sides referred to Federal and State standards and guidelines.[78] In evaluating the issues before the court, a review of these standards and guidelines is warranted.

In 1984, Congress appropriated funds for the Federal Election Commission to develop voluntary national standards to be used for computer-based voting machines. The FEC adopted the first formal set of voluntary Federal standards for computer-based voting systems in January 1990. To produce the 1990 Standards, the FEC worked with over 130 State and local election officials, independent technical experts, vendors, and Congressional staff, among others. These became known as the 1990 Voting System Standards ("VSS"). These standards and all subsequent standards and guidelines are voluntary. Each state must decide whether or not to require adherence to the guidelines. www.eac.com

When the 1990 Standards were released, there was no mechanism on a national scale by which computer-based voting systems could be tested or certified. Eventually the National Association of State Election Directors ("NASED") assumed this role. NASED is an independent organization of State election officials, and is not a governmental entity. In 1994, NASED formed the first national program to test and qualify voting systems to these standards. Through this process, vendors could submit equipment for independent testing and evaluation. NASED began by accrediting independent testing and certification facilities, labeled then as Independent Test Authorities ("ITA").

ITAs are not federal agencies. Rather, ITA was the designation devised by NASED and the FEC to describe the laboratories authorized to test the FEC standards. They were independent in the sense that they weren't directly affiliated with any election system vendors, nor were they affiliated with any State election directors. Due to rapid advancements in information and personal computer technologies, this independent testing introduced new development and implementation scenarios not contemplated by the 1990 VSS.

---

[78] Due to the length of the opinion, for convenience, the federal agencies and standards set forth in this section include the name and abbreviation.

In 1999, the FEC authorized the Office of Election Administration to revise the VSS. This resulted in the 2002 Voting System Standards, or 2002 VSS. In 2002, Congress passed HAVA, 42 U.S.C. § 1537 (b), which created a new process for improving voluntary voting system guidelines. A new federal entity, the EAC, was to oversee the process. Consistent with HAVA, the EAC established the Technical Guidelines Development Committee TGDC ("TGDC"), in cooperation with the National Institute of Standards and Technology ("NIST") to act in the public interest to assist the EAC in the development of the voluntary voting system standards and guidelines. These are characterized as "voluntary" because individual states and U.S. territories purchase their own voting systems according to state and territory specific laws and procedures.

The EAC adopted the third version of the federal voting system standards on December 13, 2005 labeling it the Voluntary Voting System Guidelines ("VVSG").[79] Voting systems submitted for testing after December 13, 2007 are tested only to the 2005 VVSG. In August 2007, the TDGC submitted draft guidelines to the EAC. One of the recommendations, software independence, was rejected. It is unclear, at this point, whether the 2007 guidelines have been adopted and, if so, what changes have been made.

According to the EAC website, there are four levels of EAC participation that each State may require regarding EAC testing and certification:

> **No Federal Requirements**: Relevant state statutes and/or regulations make no mention of any Federal agency, certification program, laboratory, or standard.
>
> **Requires Testing to Federal Standards**: Relevant state statutes and/or rules require testing to Federal voting system standards. (States reference standards drafted by the FEC, NIST, or the EAC.)
>
> **Requires Testing by a Federally-Accredited Laboratory**: Relevant state statutes and/or regulations require testing by a federally or nationally-accredited laboratory to Federal standards.
> **Requires Federal Certification**: Relevant state statutes and/or rules require that voting systems be certified by a federal agency.
>
> [www.eac.gsv (State Participation in EAC Voting System Certification

[79] This testing process continued until HAVA provided for a transitional period from the ITA system to Voting System Testing Laboratories ("VSTL"). We're now in the VSTL system.

Program).]

The experts testified that the ITA and VSTL reports have been used by many states as a sort of template for compliance, affording jurisdictions the flexibility of conducting additional testing of voting systems only to ensure compliance with particular state requirements.

During trial, plaintiffs urged the court to decommission the AVC. In part, plaintiffs suggested the court should draw a negative inference from the failure of the State to adopt the most recent federal guidelines. Given the voluntary nature of the prior standards, and now guidelines, the court rejects that notion. In a changing and complex technology environment, while adoption of new and supposedly improved guidelines may be an ultimate goal, adoption of the federal guidelines is not required.

There are a host of reasons why jurisdictions are better equipped to decide the selection of voting systems and other election administration matters. In today's economy, government must engage in a cost-benefit analysis in conjunction with the type of voting system each jurisdiction considers best suited to their needs. That is why, beginning with the 1990 standards and continuing to the present guidelines, the FEC and EAC, respectively, have made these voluntary. According to the EAC website, as of April 30, 2009, twenty states have no federal requirements, ten states require testing to federal standards, thirteen states require testing by a federally-accredited laboratory, and twelve states require federal certification. New Jersey is one of the twenty states that do not have any federal requirements. www.eac.gsv

As noted during the trial, New Jersey has not adopted the federal standards or guidelines. The Committee did have in its possession and did consider the 1994 ITA report from Wyle Laboratories ("Wyle"), a federally accredited independent laboratory, in considering a variety of enhancements presented since that time.[80] The ITA report, in essence, verifies that the AVC meets the 1990 VSS.

The court finds that the AVC has successfully been tested to be reliable under the 1990 federal guidelines as so certified by Wyle. Under the 1990 federal guidelines, voting system accuracy is

[80] The State represents the Secretary of State mandates that no voting system will be examined in New Jersey unless it has first been successfully tested by a federally accredited independent laboratory.

determined by casting approximately 297,000 consecutive votes on one machine, based on a test script. The machine passes this test if its results match the test script. The AVC has successfully tested to be accurate as such, counting all of the approximately 297,000 votes without error, as so certified by Wyle.

In addition, the election management systems, such as WinEDS, underwent additional component testing by a federally-accredited laboratory. Known as end-to-end testing, the laboratory runs a series of mock elections – from the very beginning through the end of the election cycle – of different varieties using all of the systems' voting features.

Appel's "perfection test" as to accuracy is not consistent with the standards and methodology used in the trade, federal guidelines, or statute. Furthermore, and significantly, Appel demonstrated that the AVC, in its normal operation, correctly records properly cast votes, as seen in his video demonstration accompanying the expert report.

The record reflects that the AVC was certified by the Secretary of State on August 21, 1987, following the recommendation of the Committee. No one disputes that, in 1987, at the time the AVC was certified, there were no federal standards or guidelines. As noted by several of the experts, since that time, there have been several enhancements. During the trial, the State established that since its initial approval by the Secretary of State, in 1994 the AVC was tested and passed the 1990 standards by Wyle. The 1990 federal standards required that approximately 297,000 votes be cast on the machine without error. As noted by the State's expert, it is appropriate for a state to rely on federal test results in determining whether an update to an already certified voting system requires full recertification.

Since 1987, there have been a number of modifications and/or enhancements. It is also true that none of these were subject to a full re-certification. N.J.S.A. 19:53-4 provides that "any improvements or changes" that do not impair the accuracy or efficiency of such a machine shall not require any reexamination. Plaintiffs assert that due to the nature of the enhancements, full recertification was required. Defendants rely on N.J.S.A. 19:53-4 for the proposition that none of the enhancements raised issues regarding the accuracy or efficiency of the voting system.

Clearly, for voting systems that involve a computer based system, the court finds the present

composition of the Title 19 Committee in violation of the statutory requirement that the Committee be composed of two mechanical experts.[81] As will be noted later in this opinion, due to the current composition of the Committee, the court finds that the enhancements/modifications should be evaluated by a newly-constituted Title 19 Committee, or if the Legislature deems it appropriate, by a new entity to review voting systems.

D.

TRIAL FINDINGS

On January 27, 2009, when the trial commenced, the State had not implemented the VVPAT. Six weeks later on March 6, 2009, the statutory deadline was extended indefinitely. It is undisputed that the DRE voting system has been in use since as early as 1979. While this opinion will discuss important steps the State must take to address certain issues raised during trial, not one witness presented evidence that the AVC, outside of a controlled academic setting, has ever been hacked. In fact, other then the "option switch bug," the expert witnesses and county election officials agreed that, absent purposeful and criminal intrusion by an outsider or insider, the AVC records votes cast and produces accurate results.[82] N.J.S.A. 19:48-1 and N.J.S.A. 19:53A-3.

The court agrees with defendants that the claims regarding security risks of the AVC are not consistent with the State's over fifteen year record of successful elections using this voting system. The record is void of any evidence to establish that any election has ever been compromised due to the fraudulent manipulation of an AVC voting system. As noted by defendants, "if the mere physical or technological possibility of criminals to supersede government activity were to warrant strict scrutiny,

[81] The definition of a "mechanical expert" may differ depending on the type of voting system used: i.e., the skills required to inspect and certify a mechanical lever machine as opposed to an electronic voting system machine.

[82] The option switch problem occurred when a board worker pressed an inappropriate sequence of buttons on the option switch panel. This problem was discovered in the February 2008 primary. The problem, once identified, was corrected by placing a plastic shield over the operator panel. In the primary elections held since that time, no problems have been reported.

then many regulatory decisions, both in and out of the election context would not survive constitutional review." Def. Br. at 17, citing DeShaney v. Winnebago Cty. Soc. Servs. Dept., 489 U.S. 189 (1989)(holding that states are not constitutionally required to "protect the life, liberty and property of its citizens against invasion by private actors.).

Interestingly, absent the hypothetical situation of criminal access and the installation of fraudulent software, plaintiffs' own expert did not find any malicious software in the source code or any irregularities that would result in the AVC failing to count votes as cast.

While the AVC is not a perfect voting system and there are serious issues that remain to be addressed, based on the evidence adduced at trial, the court finds the following:

> (1) No AVC has ever been demonstrated to have been hacked, other than in an academic setting, in this State or any other state.
>
> (2) There has never been a demonstrated incident of an attempted attack or a verified attack of any AVC voting system in the United States since its use began at least as early as 1979.
>
> (3) Replacement of the AVC ROM chip with a fraudulent ROM chip is not a realistic risk. The systematic one-by-one replacement of ROM chips by an intruder, or even an insider, would require mechanical and physical changes to each and every machine.
>
> (4) It would be extremely unlikely that one could replace DRE firmware with fraudulent firmware while leaving no detectable evidence of that under real election conditions.[83]
>
> (5) The tamper-evident seals and locks serve as a deterrent. While these seals may be visually inspected by election officials and their serial number checked against records upon the voting machines' return to the warehouse post-election, the State does not have an adequate inspection protocol.
>
> (6) The new seals used in New Jersey will have serial numbers to aid in identifying tampering. The State must take steps to require election officials to: (1) check and record the serial numbers; (2) adopt a uniform seal-use inspection protocol; and (3) provide inspectors with adequate training.

[83] The three election representatives in charge of the handling and storage of the voting machines each outlined the measures taken to secure the voting machines. Given the alarm systems in place, limited password or key access, and precautions undertaken by the election representatives who testified, outsiders cannot realistically perpetrate such an attack at voting machine warehouses.

(7) While insiders may pose a security risk, this is true with all voting systems; it is not a risk unique to the AVC or any other DRE or voting system.[84]

(8) The record demonstrates that the DRE is a complicated system. Thus, the creation of a Trojan horse – in which a voting machine outwardly appears to the user to be using the legitimate program, but is secretly doing other things unseen by the user – is not a trivial process.[85]

(9) The technical barriers to producing fraudulent firmware, and the necessary step of reverse engineering the source code, are substantial.[86]

(10) The notion that fraudulent firmware can continue to operate, as anticipated, for future elections, is completely unrealistic.[87]

11. Security vulnerabilities are present, to some degree, in every voting system. There is simply no such thing as a voting system that is impossible to manipulate.[88]

12. Viruses do not present a legitimate risk to the AVC. The notion that some kinds of fraudulent firmware can automatically propagate themselves from one AVC to another is purely hypothetical.

13. The viral mode theorized by plaintiffs' expert through the use of the daughterboard is fictional.[89]

---

[84] As a result, this concern does not warrant banning the use of the AVC. This is particularly true where plaintiff offered no proof of any "insider" manipulation.

[85] Further, a hacker without the benefit of the source code would need to reverse engineer the ROM chip to create a fraudulent program in order to know what to change.

[86] It has taken world-renowned security experts substantial time to perpetrate such hacks in a laboratory setting.

[87] No one knows how each future election will be set-up and no one can anticipate changes in the law, changes in the outcome of ballot rotations affecting the election setup, changes in the ballot formation, changes in the demographics of the jurisdiction or changes in the rotations of machines in different jurisdictions.

[88] As a result, in evaluating the reasonableness of a particular voting system, the court cannot apply the "perfection" standard proposed by plaintiffs' experts. Rather, the appropriate standard is whether a particular voting system can be safely used under normal election conditions. This is the standard adopted in New Jersey and in other states.

[89] Even if this was possible, the theoretical attacks could only cause votes to be altered if they had been cast by an audio voter and could only affect the motherboard into believing the machine was in a state ready for voting, requiring it to be taken out of service. As reference, only four people voted by way of audio during the February 5, 2008 Presidential primary in Bergen County, New Jersey's most populous county.

14. A WinEDS enabled computer should never be connected to the Internet.

15. The State's experts testified that both anti-virus software and hardening measures should be added to WinEDS enabled and Election Central computers.

16. There is no documented incident where anyone has ever manufactured a fake AVC Z80 chip containing fraudulent firmware.

17. There is no documented incident where any fake microprocessor was ever inserted into an AVC.

18. The court rejects the so-called "perfection standard."[90]

19. While Appel supports the use of optical scan voting systems, he has never conducted an evaluation of the security or any other aspect of this type of equipment.

20. Installing fraudulent Z80 chips would take hundreds of hours to do, and presents the same problems with breaking in and replacing ROM chips on an individual machine-by-machine basis.

21. Appel never demonstrated that the data in an AVC results cartridge could be altered.[91]

22. Daughterboard manipulation by direct access does not present a serious risk.[92]

23. The presence of third-party software does not constitute a serious risk.

24. There is no evidence that the AVC, in its normal state: (1) has design flaws that cause votes to be lost; (2) encourages voter and poll worker error; or (3) permits fraudulent manipulation.

---

[90] Instead, the standard should exclude systems that are so insecure as to be easily tampered with under normal conditions. It should never impose a requirement of absolute security or complete protection against tampering, which would be impossible to achieve.

[91] Even if possible, these results cartridges are only used to produce unofficial results of an election. The results data on a results cartridge can also be verified by comparing it with the results data on the original paper produced directly from the machine at the polling places and signed by the poll workers on election night.

[92] There is no serious risk inasmuch as: (1) audio cartridges are securely distributed and installed at the warehouses; (2) the cartridges are protected by tamper-evident seals installed on the audio cartridge slot on the AVC; (3) any intrusion could only affect audio votes; and (4) manipulation would require deliberate, individual intrusion into each voting machine.

25. The option switch issue, triggered when a poll worker pressed an inappropriate sequence of buttons on the operator panel, has been corrected.[93]

26. The user interface provides several indications to voters that an AVC is activated.

27. The AVC indicates under-votes and meets the 2002 federal guidelines. The AVC indicates to the voter when no selection, or an insufficient number of selections, has been made in a contest.

28. The AVC permits write-in votes to be changed after pressing enter but before pressing the "Cast Vote" button. Should the voter wish to review or correct a write-in after pressing the enter button, the voter applies the same procedure used for obtaining a replacement optical scan ballot.

29. WinEDS is equipped to insert names with tildes on a summary report.

30. The candidate ID issue will only occur when there are 1,000 candidates on a county's ballot. It does not affect vote totals. This rare occurrence is easily corrected.

31. The software design of the AVC does not cause any votes to be miscounted.

32. While two graduate students reverse engineered 20 percent of the firmware of the version 5 AVC, reverse engineering is a complex process.

33. To create a vote-stealing program, the attacker would require the source code or its functional equivalent to create the program.

34. Appel did not remove the Z80 from the circuit board on the voting machine, or design fraudulent firmware to modify the Z80, and acknowledged he had never done so.

35. Appel testified that it would take at least a month to develop a fraudulent Z80 to cheat in elections.[94]

While the trial addressed the paperless AVC, both Appel and Shamos testified regarding precinct-based optical scan voting systems. This type of voting system uses paper ballots and has a computer that reads and tabulates the ballots. Appel strongly endorses precinct-optical scan voting systems and testified

[93] The issue only affected the secondary report of party tallies, or party turnout totals, not the candidate tallies. Therefore, it did not cause a single vote to be lost or not counted.

[94] Appel did not reverse engineer the daughterboard firmware.

that experts in the scientific community do as well.

Like a DRE, the precinct-based optical scan machine has a motherboard, a microprocessor, firmware, and software. According to Shamos, the hardware and software components of precinct-based optical scan systems are vulnerable to corrupt manipulation in several different ways. First, if a corrupted precinct-based optical scan system is used during a recount, the result would be corrupted. Second, if the ballots are recounted by hand, handling could affect the integrity of the recount. Third, unlike a DRE, no computer experience or technical skills are required to tamper with paper ballots. Fourth, the firmware on precinct-based optical scan voting systems may be replaced with fraudulent firmware to produce corrupt vote totals just as is theorized with DREs. In fact, Shamos noted that replacement is much easier on a precinct-based optical scan system because its firmware is simpler and the source code is much shorter and hence easier to reverse engineer than that of a DRE. Fifth, the precinct-based optical scan machine oftentimes produces a ballot in which the officials are unable to establish voter intent. By contrast, it is unambiguous whether a candidate has been selected or not on DRE voting systems.

The record reflects that Shamos has performed more than 120 voting system certification examinations. Appel has never conducted a voting system certification examination. Appel did not conduct a comparable study or review of an optical scan voting system.

Shamos testified that precinct-based optical scan voting systems are not more secure than DREs and, in fact, many of the vulnerabilities present in these systems are far worse than in DRE systems. To support this, Shamos testified that in every election cycle in the United States in which precinct-based optical scan systems have been used, ballots have been lost.

The role of this court is not to determine the accuracy or reliability of precinct-based optical scan voting systems. Nor has the court identified all of the alleged infirmities described by Shamos. Suffice it to say, government and election representatives in this State may deem it appropriate to review this testimony as part of its evaluation of how to proceed in the future. Finally, Shamos testified that the complaints by Appel; to wit security, audits, and viruses, even if accurate, would also apply to DREs with VVPAT and optical scan voting systems.

E.

STATUTORY REQUIREMENTS FOR VOTING MACHINES

The complaint includes both constitutional and statutory claims. Since the two are inextricably intertwined, the court rejects the notion that only the constitutional claims remain. "Legislative enactments are presumed to be valid and the burden to prove invalidity is a heavy one." Bell v. Twp. of Stafford, 110 N.J. 384, 394 (1988). The Legislature has broad discretion in determining the parameters of legislation. Brown v. State, 356 N.J. Super. 71 (App. Div. 2002); Harvey v. Essex Cty. Bd. of Freeholders, 30 N.J. 381, 390 (1959). "In considering constitutionality of legislation courts do not weigh its efficacy or wisdom." State Farm Mut. Auto. Ins. Co. v. State, 124 N.J. 32, 45 (1991).

In the case at bar, N.J.S.A. 19:48-1 allows "any thoroughly tested and reliable voting machines to be adopted, rented, purchased or used." Ibid. Pursuant to N.J.S.A. 19:48-2, the examination of voting machines and their certification of approval are conducted by the Secretary of State. N.J.S.A. 19:48-2 states in pertinent part that:

> The certificate of approval, or a certified copy thereof, shall be conclusive evidence that the kind of machine so examined complies with the provisions of this subtitle, except that the action of the Secretary of State in approving such machine may be reviewed by the Superior Court in a proceeding in lieu of prerogative writ.
>
> [Ibid. (emphasis added).]

Although N.J.S.A. 19:48-2 states that the findings regarding voting machines are conclusive, the statute provides a mechanism for review by the Superior Court. Therefore, the appropriate standard normally would be to assign a rebuttable presumption in favor of the Secretary of State's approval, thereby placing the burden on plaintiffs in this case to prove otherwise. Based on the reasons set forth below, however, this court finds that given the inadequacies in the composition of the Committee, the Secretary of State is not entitled to that presumption of validity.

N.J.S.A. 19:48-1, entitled "Requirements for voting machines," provides that "any 'thoroughly tested and reliable' voting machines may be used in an election." While not defined in any one section, paragraphs (a) through (n) identify the requirements necessary to meet this standard. Paragraphs (d), (f),

and (h), referred to in the complaint, all relate to the accuracy of the voting machine. Paragraph (d) provides that the machine "shall permit the voter to vote for as many persons for an office as he is lawfully entitled to vote for, but no more." Paragraph (f) provides that "it shall permit the voter to vote for or against any question he may have the right to vote on, but no other." Paragraph (h) requires all voting machines to "correctly register or record and accurately count all votes cast for any and all persons, and for or against any and all questions."

In N.J.S.A. 19:53A-3, entitled "Requirements for Electronic Voting Systems," paragraphs (a) through (h) identify the requirements necessary for each electronic voting system used in this State. The requirement for each voting system to produce a VVPAT, as noted heretofore, has been indefinitely suspended. Similar to paragraph (h) in N.J.S.A. 19:48-1, paragraph (h) of N.J.S.A. 19:53A-3, referring to each electronic voting system, provides "when properly operated [the voting system] shall record correctly and count accurately every vote cast, including all over-votes or under-votes and all affirmative votes or negative votes on all public questions and referenda." Paragraph (g) provides that every electronic voting system shall "be suitably designed for the purpose used, of durable construction, and may be used safely, efficiently, and accurately in the conducting of elections and counting ballots."

For the reasons set forth in the court's findings, based on the extensive testimony and evidence in this case, the court is satisfied that the AVC meets these standards. There is simply no evidence to conclude that absent complete access, coupled with malicious intent to alter the results of an election, the voting machines have failed to correctly and accurately count every vote cast. The court rejects the notion that the AVC is not reliable because it cannot be secured from tampering. As noted by the State's expert, reliability and security are two separate concepts.[95]

---

[95] Security is addressed in N.J.S.A. 19:48-1a(i)(requiring a protective counter); N.J.S.A. 19:53A-3(g)(requiring that the system may be safely used in elections); and N.J.S.A. 19:34-11(criminalizing fraudulent voting), among other provisions. Design is addressed in N.J.S.A. 19:48-1(a)(a)(requiring that voter privacy be secured); N.J.S.A. 19:48-1a(o)(banning the use of mechanical levers and punch cards); N.J.S.A. 19:53A-3(g)(requiring durable construction), among other provisions; and N.J.S.A.19:48-1(j)(requiring the locking, sealing and custody of the AVC after elections to prevent post-election operation).

Despite an extended period of time, from the inception of the litigation in October 2004 to the last day of trial on May 11, 2009, plaintiffs have not established any evidence of tampering of an AVC used in an actual election in this State. Instead, plaintiffs were only able to demonstrate a single manipulation in a laboratory setting. Clearly, the court cannot conclude that a voting system that can be manipulated under artificial laboratory conditions should be decommissioned.

Plaintiffs also allege that use of the AVC violates the statutory guidelines for recounts found in N.J.S.A. 19:28-1 et seq. Plaintiffs argue that by producing no evidence of voter intent that can be independently verified, paperless DRE voting systems violate the law. This is simply contrary to the evidence adduced at trial. Given the redundant memory of the AVC and the testimony of the State's witnesses, there is no evidence to support a failure to adhere to the statutory requirements under Title 19.

F.

CONSTITUTIONAL CLAIMS

As noted heretofore, the Appellate Division directed this court to conduct regular reviews to monitor compliance with the VVPAT legislation. Specifically, the Appellate Division held that in the event that the State did not implement the VVPAT legislation, this court's review should be limited to plaintiffs' constitutional claims. Recent legislation has delayed the implementation of the VVPAT indefinitely.

Plaintiffs first assert that the use of the AVC violates this State's citizens' right to vote:

> Every citizen of the United States, of the age of 18 years, who shall have been a resident of this State and of the county in which he claims his vote 30 days, next before the election shall be entitled to vote for all officers that now are or hereafter may be elective by the people, and upon all questions which may be submitted to the vote of the people.
>
> [N.J.Const. Art. II, Sec. I, para. 3.]

To support this notion, plaintiffs assert that use of the AVC violates the fundamental right to vote because it can easily be made to subvert voter intent. Plaintiffs argue that: (1) the vote-stealing program was easy to make; (2) a fraudulent Z80 that cheats in elections is easy to make and almost impossible to detect; and (3) the proposed security measures cannot protect against tampering.

Second, plaintiffs assert a violation of the Equal Protection guaranteed by the New Jersey Constitution. Relying on the recount requirements, plaintiffs argue that DRE voters have no assurance that their votes will be treated the same as votes cast by absentee and emergency paper ballots resulting in unequal treatment. The Equal Protection guaranteed by the New Jersey Constitution provides:

> [a]ll persons are by nature free and independent, and have certain natural and unalienable rights, among which are those of enjoying and defending life and liberty, of acquiring, possessing, and protecting property, and of pursuing and obtaining safety and happiness.
>
> [N.J. Const. Art. I, Sec. 1.]

The court rejects the notion that vote-stealing programs are easy to make and that a fraudulent Z80 that cheats in elections is easy to make and almost impossible to detect. The court also finds that there is no system immune from potential tampering in the face of criminal activity.

When faced with a constitutional challenge, a statute is presumed to be constitutional. To overcome this presumption, the plaintiff must demonstrate that there are no conceivable grounds to support its validity. Brown, supra. 356 N.J. Super. at 79-80. This deferential standard is rooted in separation of power principles, which are even stronger when a court is asked to invalidate, rather than simply interpret, a legislative intent. Out of respect for the democratic process, and in recognition of the legislature's status as a co-equal branch of government, statutes under attack are "entitled to great weight by the courts." N.J. Sports & Exposition Auth. v. McCrane, 119 N.J. Super. 457, 474 (Law Div. 1971), aff'd, 61 N.J. 1 (1972)(quoting Roe v. Kervick, 42 N.J. 191, 229-30 (1964)). Significantly, courts will not second-guess the legislature's policy decisions regarding economic, social and philosophical issues. Brown, supra, 356 N.J. Super. at 80 (quoting Reiser v. Pension Comm'n of Passaic City, 147 N.J. Super. 168, 183 (Law Div. 1976)).

While the right to vote is deemed as central to our democratic system, it is equally widely accepted that States must actively participate in regulating elections to ensure their integrity and fairness. Burdick v. Takushi, 504 U.S. 428, 433, 112 S.Ct. 2059, 119 L.Ed. 2d 245 (1992); New Jersey Conservative Party, Inc. v. Farmer, 332 N.J. Super. 278, 287 (Ch. Div. 1999).

While it is beyond question that the right to vote is fundamental, it is also well-settled that states are entitled to broad leeway in regulating elections to ensure that they are carried out in a fair, orderly, and efficient manner. Yick Wo v. Hopkins, 118 U.S. 356, 370, 6 S.Ct. 1064, 30 L.Ed. 220 (1886); Wurtzel v. Falcey, 69 N.J. 401, 403 (1976). Applying these basic principles, courts hearing constitutional challenges to an electoral regulation must apply a balancing test. In Farmer, supra, 332 N.J. Super. at 287, the court relied on the analysis set forth by the Supreme Court of the United States:

> [w]e weigh the character and magnitude of the burden the State's rule imposes on those rights against the interests the State contends justify the burden necessary. Regulations imposing severe burdens on plaintiffs' rights must be narrowly tailored and advance a compelling state interest. Lesser burdens, however, trigger less exacting review, and a State's important regulatory interests will usually be enough to justify reasonable nondiscriminatory restrictions. No bright line separates permissible election-related regulation from unconstitutional infringements.
>
> [Ibid., quoting Timmons v. Twin Cities Area New Party, 520 U.S. 351, 358, 117 S.Ct. 1364, L.Ed. 2d 589 (1997).]

Applying this standard, the Farmer court dismissed plaintiffs' complaint. In doing so, the court acknowledged the comprehensive opinion by Judge Ward in New Alliance Party v. New York Bd. of Elections, 861 F. Supp. 282 (1994). In New Alliance Party, plaintiff filed an action against the State Election Board seeking a declaration that an election law was unconstitutional because it denied independent political parties from being listed in the first place on an election ballot. New Alliance Party recognized that "because constitutional protection is dependent not on the question of the voting rights' fundamental nature but on the extent to which a restriction impinges upon exercise of those rights, a balancing test is used for distinguishing valid from invalid restrictions." Id. at 24.

The analysis is, in essence, akin to the balancing test employed in fundamental rights claims under the New Jersey Constitution. See Greenberg v. Kimmelman, 99 N.J. 552, 567 (1985). While Farmer, New Alliance Party, and Timmons addressed ballot-type issues, the distinction between a severe restriction and a reasonable nondiscriminatory restriction is significant. These cases are consistent with the cases that have addressed the use of electronic voting machines.

In Burdick, the Court held that Hawaii's prohibition on write-in voting in the State's primary and general elections did not impose an unconstitutional burden on the rights of the State's voters under the Federal Constitution's First and Fourteenth Amendments. 504 U.S. at 428. Significantly, the court differentiated between the different burdens a trial court should apply. The court held:

> Under this standard, the rigorousness of our inquiry into the propriety of a state election law depends upon the extent to which a challenged regulation burdens First and Fourteenth Amendment rights. Thus, as we have recognized when those rights are subjected to severe restrictions, the regulation must be narrowly drawn to advance a state interest of compelling importance. But, when a state election law provision imposes only reasonable, nondiscriminatory restrictions upon the First and Fourteenth Amendment rights of voters, the State's important regulatory interests are generally sufficient to justify the restrictions.
>
> [Id. at 434.]

Based on the above, the Court applied the reasonableness standard in considering plaintiff's challenge to Hawaii's ban on write-in ballots.

States may impose time, place and manner restrictions on elections under Article I §4, cl. 1 of the United States Constitution. Burdick, supra, 504 U.S. at 433 (internal citations omitted). States may thus regulate their elections "to ensure orderly, rather than chaotic, operation of the democratic process." Farmer, supra, 332 N.J. Super. at 287. (internal quotations omitted). Indeed, the Burdick court recognized that "substantial regulation" is likely necessary to accomplish this goal. 504 U.S. at 433.

The Court in Burdick further acknowledged that any regulation on elections will necessarily "impose some burden upon individual voters." Id.; see also Timmons, supra, 520 U.S. at 358. The question, then, becomes what standard applies in evaluating the constitutionality of a given election regulation or limitation. There is no litmus test to apply in order to reach a conclusion; rather, the United States Supreme Court has enunciated a balancing test to be applied on a case-by-case basis. See Timmons, supra, 520 U.S. at 359; Burdick, supra, 504 U.S. at 434; and Anderson v. Celebrezze, 460 U.S. 780, 789, 103 S.Ct. 1564, 75 L. Ed. 2d 547 (1982).

The flexible test requires the court to first consider "the character and magnitude of the asserted injury to the rights protected by the First and Fourteenth Amendments that the plaintiff seeks to

vindicate." Burdick, supra, 504 U.S. at 434 (citing Celebrezze, supra, 460 U.S. at 789). These rights are then to be weighed against the "precise interest put forward by the State as justifications for the burden imposed" by the relevant regulation or rule. Ibid. Finally, the court should take into consideration the "extent to which [the State's] interests make it necessary to burden the plaintiff's rights." Ibid.

The Burdick court enunciated two more specific standards; one concerning a regulation that results in "severe" restrictions, and the second concerning only "reasonable, nondiscriminatory restrictions" on voters' rights. Ibid. (quoting Norman v. Reed, 502 U.S. 279, 289, 112 S.Ct. 698, 116 L.Ed. 2d 711 (1992)). With respect to the first, if a regulation "severely" infringes upon the constitutional rights of voters, then heightened scrutiny applies and the regulation must be narrowly tailored to advance a compelling State interest. Ibid. When there is only a "reasonable, nondiscriminatory restriction" on such rights, though, lesser scrutiny is applied and the "State's important regulatory interests are generally sufficient" justification for the restriction. Ibid. (quoting Celebrezze, supra, 460 U.S. at 788).

The New Jersey Supreme Court has similarly distinguished between those regulations which place severe restrictions on an individual's rights and those regulations which result in reasonable restrictions. Specifically, in Greenberg v. Kimmelman, supra, 99 N.J. at 552, the court discussed the different tiers and levels of review involved in a federal equal protection analysis. The Court found that the standard of review will vary based upon the effect of the governmental regulation in question on the affected right. That is, "[w]hen the effect on a right, even a right that is fundamental, is indirect or insubstantial the Court has applied the rational basis test and upheld a legislative classification." Id. at 565. By way of example, the court looked at two cases involving the right to marry, wherein a rational basis standard was employed when the statute at issue had only an indirect effect on the decision to marry, Califano v. Jobst, 434 U.S. 47, 53-58, 98 S.Ct. 95, 54 L.Ed. 2d 228 (1977), and a strict scrutiny standard was applied when the statute directly and substantially interfered with the right to marry. Zablocki v. Redhail, 434 U.S. 374, 387, 98 S.Ct. 673, 54 L.Ed. 2d 618 (1977).

New Jersey courts have had subsequent opportunities to apply this test, and have rejected the notion that the proper standard is automatically strict scrutiny, a conclusion consistent with the standard

set forth in Celebrezze and Burdick. See Council of Alternative Political Parties v. New Jersey, 344 N.J. Super. 225 (App. Div. 2001). The level of scrutiny instead "depends on the nature of the interest impinged on or burdened by the restriction and the extent of the burden." Ibid.; see also Farmer, supra, 332 N.J. Super. at 288 (citing New Alliance Party v. N.Y. State Bd. of Elections, supra, 861 F. Supp. at 295); and Hartman v. Covert, 303 N.J. Super. 326, 331-332 (Law Div. 1997).

In Schade v. Maryland State Bd. of Elections, 401 Md. 1 (2007), the appellants, registered voters and candidates for public office, were granted certiorari to challenge the Circuit Court, which denied their request for a preliminary injunction. On appeal, the court held that the State Board of Elections acted reasonably in purchasing and certifying the electronic voting system. Like here, appellants sought relief in the form of decertification. Also, electronic voting machines have been used in Maryland since 1996.

Precipitated in part by the 1994 Gubernatorial Election, which was a very close election for governor, involving problems with vote counting accuracy and conducting recounts, Maryland began exploring ways to improve its voting process. As part of this effort, a series of commissioners were appointed to study the election process in Maryland. As a result of that examination, it was suggested that elections in Maryland needed to be modernized and that uniformity should be the benchmark for any such efforts. The Governor formed a special committee on Voting Systems and Election Procedures in Maryland (the "Special Committee"). The Special Committee issued a report in February 2001, recommending that Maryland adopt a uniform statewide voting system for both the polling places and for absentee voting.

In Schade, appellants' expert witnesses applied the "perfection" standard also used by Appel. In this standard, the expert testified that it was impossible for a paperless electronic voting machine to protect the security and accuracy of a voting process. As a solution, the expert proposed a voter-verified audit trail. Id. at 18-19.

In Schade, the defense called Shamos, the same expert called by the State in the case before this court. Shamos testified that a voting system does not exist that is impervious to fraud. Rejecting the "perfection" standard, Shamos applied a reasonableness standard. Shamos testified paper-based ballot

options, i.e., paper ballots and optical scan systems, were less secure, not more secure than DRE machines, and that paper ballots and optical scan systems were not remedies, but instead alternatives, at best, to the alleged vulnerabilities in DRE machines." Id. at 23-24.

On appeal, the Court held that neither the trial court nor the Circuit Court erred in giving more weight to the testimony of Shamos over the testimony of plaintiffs' experts. The Court held the Circuit court did not abuse its discretion in its consideration and balancing of the factors pertinent to the review of the appellants' request for injunctive relief. Id. at 37.

Shamos disagreed with the notion that a VVPAT was necessary. In fact, he explained that "a paper trail does not solve the problems that are alleged to affect or afflict the DRE machines." Id. at 23. Instead, he noted that "a paper audit trail would simply restore us to the 1850s when all manner of chicanery was performed through manipulation of pieces of paper. And we don't have any better technology now than we had 150 years ago for assuring the security of pieces of paper." Ibid. In fact, his testimony in the matter before this court is nearly identical.

Like in Schade, Shamos testified in the case before this court that paper-based ballot options, i.e., paper ballots and optical scan systems, were less, not more, secure than DRE machines, and that paper ballots and optical scan systems were not remedies, but instead alternatives, at best to the alleged vulnerabilities in DRE machines.

Furthermore, as in Schade, Shamos testified before this court that optical scan systems are not, and have never been, subjected to the extensive testing that has been performed on DRE machines.

In Schade, the Supreme Court addressed appellants' argument that the Circuit Court's wholesale adoption of Shamos' testimony was in error. The Court noted:

> In other words, evidence offered by the parties was conflicting to some degree in many respects. Accordingly, the responsibility for resolving those conflicts lies with the Circuit Court, as it is in the best position, a position far more superior that that of an appellate court, to evaluate and weigh such evidence.
> [Id. at 35.]

In Wexler v. Anderson, 452 F.3d 1226 (11th Cir. 2006), plaintiffs filed suit alleging that the use of touch-screen voting systems that did not produce a paper record of votes violated the Due Process Clauses of the Fifth and Fourteenth Amendments. Plaintiffs argued that: (1) manual recount procedures, which varied by county according to voting system, accorded arbitrary and disparate treatment to voters; and (2) voters were not accorded equal treatment because those residing in optical scan counties would have an opportunity to have their residual votes reviewed whereas those residing in touch-screen counties would not. The United States District court for the Southern District of Florida ruled for the state officials. An appeal followed and the district court decision was affirmed. The Supreme Court denied certiorari.

In Weber v. Shelley, 347 F.3d 1101 (9th Cir. 2003), plaintiff filed suit alleging that the lack of a voter-verified paper trail in the county's newly installed touch screen voting system violated her rights to equal protection and due process. Plaintiff argued that: (1) the right to vote is infringed when the ease with which ballots can be manipulated is greater than the ease with which the manipulation can be detected; and (2) the court misapplied Burdick by failing to subject paperless touch screen systems to strict scrutiny. Id. at 1104-5. The United States District court for the Central District of California ruled for the State officials. An appeal followed.

On appeal, the appellate court affirmed the holding that States are entitled to broad leeway in enacting reasonable, even-handed legislation to ensure that elections are carried out in a fair and orderly manner. The court held:

> The use of touch-screen systems is not subject to strict scrutiny simply because this particular balloting system may make the possibility of some kinds of fraud more difficult to detect. Rather, the question is whether using a system that brings about numerous positive changes (increasing voter turnout, having greater accuracy than traditional systems, being user friendly, decreasing the number of mismarked ballots, saving money, etc.) but lacks a voter-verified paper ballot, constitutes a "severe" restriction on the right to vote.
>
> [Id. at 1106.]

The court recognized that no balloting system is perfect. "[I]t is the job of democratically-elected representatives to weigh the pros and cons of various balloting systems. So long as their choice is

reasonable and neutral free, it is free from judicial second guessing." Id. at 1107. The question is whether the State made a reasonable, politically neutral and nondiscriminatory choice to certify touch screen systems as an alternative to paper ballots. Nothing in the Constitution forbids this choice. Ibid.

In Mills v. Shelby County Election Comm., 218 S.W. 3d 33 (Tenn. App. 2006), Mills, a voter, filed suit under the Tennessee Declaratory Judgment Act against Shelby County, asserting that legislation authorizing the use of electronic voting machines in some jurisdictions violated the State Constitution. Plaintiff sought to have the trial court declare that the State must use a system of voter verified, tangible paper ballots that are capable of being placed by the voters into a ballot box for later tabulation. The State moved to dismiss. The trial court dismissed the complaint with prejudice. An appeal followed.

On appeal, the court rejected the notion that the use of electronic voting machines, as opposed to paper ballots, created an inequality in voting. The court held "the use of 'free and equal' in the Tennessee Constitution refers to the rights of suffrage and not to the logistics of how the votes are cast." Id. at 40-41. The court recognized: (1) the well settled authority that it is for the State to control the conduct of elections; Id. at 41; (2) the absence of evidence to support the notion that a paperless touch screen voting system severely restricted the right to vote, Ibid; and (3) that no ballot system is perfect. Id. at 42 (citing Weber, supra, 347 F.3d at 1106).

A related, potential threshold issue concerns the limits of proper judicial involvement in the election process, an inherently legislative and executive endeavor. See Gormley v. Lan, 88 N.J. 26 (1981) (Handler, J. concurring and dissenting)(agreeing that the court properly deemed insufficient an explanatory statement on a ballot, but disagreeing with a portion of the court's suggested – but not ordered – alternative language for the statement as overstepping its authority). In New Jersey, it is not controversial that, generally, legislative enactments are presumed valid and that the legislative judgments deserve deference from the judiciary. Roe, supra, 42 N.J. at 191; State Farm Mutual Automobile Ins. Co. supra, 124 N.J. at 32. "A legislative act will not be declared void unless its repugnancy to the constitution is clear beyond reasonable doubt." Gangemi v. Berry, 25 N.J. 1 (1957). The burden on someone

attempting to invalidate a legislative act is thus very heavy. Bell v. Twp. of Stafford, supra, 110 N.J. at 384 (1988).

When it comes to voting machines, as a preliminary matter, some courts in other jurisdictions have begun by acknowledging that there is no such thing as a perfect system, impervious to flaws; or at least that a particular voting machine at issue is subject to some level of vulnerability. Schade, supra, 401 Md. at 22; Ford v. County of Carlisle, 361 S.W. 2d 757, 759 (Ky. Ct. App. 1962); See also Weber, supra, 347 F.3d. at 1107 (9th Cir. 2003). This sentiment applies to technologically advanced voting systems as well as traditional paper ballots, which can result in both under-votes and over-votes, as well as so-called "hanging chads." Wexler v. Lapore, 878 So. 2d 1276, 1282 (Fl. Ct. App. 2004) (upholding the certification of the challenged touchscreen voting system); Anderson, supra, 452 F.3d. at 1226; Weber, supra, 347 F.3d. at 1101; Favorito v. Handel, 684 S.E. 2d 257 (Ga. 2009); and Soubirous v. County of Riverside, 2006 Cal. App. Unpub. LEXIS 1218.

Some such cases arose in the context of claims that a particular voting machine is subject to so many or such serious potential problems that they rise to an infringement on the right to vote. Anderson, supra, 452 F.3d at 1227; Weber, supra, 347 F.3d at 1102. In these cases in the 11th and 9th Circuits respectively, the courts found that potential or theoretical problems with touch screen voting machines were insufficient to implicate constitutional claims. Wexler, supra, 452 F.3d. at 1232; Weber, supra, 347 F.3d. at 1105. The Weber court took it a step further, beginning by acknowledging an array of potential problems in the particular voting machine at issue, the AVC Edge System used without a VVPAT. Ibid. The court then noted that there was "no indication that the [system]… is inherently less accurate, or produces a vote count that is inherently less verifiable, than other systems." Ibid. Similarly, the Wexler court addressed the "mere possibility" that voters using the challenged touch screen system would be burdened by the lack of an opportunity to have certain votes counted manually, as voters in optical scan counties had. 452 F.3d. at 1232. The court was not persuaded that this potentiality merited a constitutional application. Ibid.

At issue in Soubirous was the AVC Edge Touch Screen Voting System, used without a VVPAT. The plaintiffs there claimed, among other things, that the voting data stored electronically in those machines is "susceptible to manipulation or degradation during the process of recording and the process of transmission." Soubirous, 2006 Cal. App. Unpub. LEXIS at 4. At the time of the decision, the legislature had recently changed the law to require that all DRE voting systems used in the state be used with printers to print a paper record of each electronic ballot. Id. at 59. This change in the law rendered this particular claim moot, as it was a request for documents founded upon the allegation that the violations would continue into the future. Ibid.

In Favorito, supra, 684 S.E. 2d at 257, plaintiffs filed a multi-count complaint for declaratory judgment, injunction, and mandamus against the Secretary of State, the Governor of Georgia, and the Georgia State Election Board challenging the use of the DRE equipment. On cross-motions for summary judgment, the trial court granted defendants' motion and plaintiffs appealed.

On appeal, appellants argued: (1) the state's use of the DRE denied them equal protection under the Federal and State Constitutions and the fundamental right to vote under the due process clause of the Fourteenth Amendment; (2) the trial court erred by failing to recognize that voting is a fundamental right and improperly applied a "rational basis" test instead of a "strict scrutiny" test; (3) the fundamental right to vote has been injured because the recording, counting, and retention of their votes, unlike paper ballots, were not properly protected either by an independent audit trail or by county and state tabulators which can prevent fraudulent manipulation; and (4) the DRE voting system fails to assure that each vote is accurately counted, and thus fails to comply with the statutory requirements.

The court rejected all four arguments. The court held that unless governmental action infringes upon a fundamental right or the complaining party is a member of a suspect class, a substantive due process or equal protection challenge is examined under the rational basis test. While "the right to vote is fundamental, forming the bedrock of our democracy," the court held that states are entitled to broad leeway in enacting reasonable, even-handed legislation to ensure that elections are carried out in a fair

and orderly manner. Favorito, supra, 684 S.E. 2d at 257; Anderson, supra, 452 F.3d at 1226, 1232. See also Weber, supra, 347 F.3d at 1105.

Similarly, the court rejected the notion that their fundamental right to vote was being injured because the recording, counting and retention of their votes, unlike paper ballots, are not being properly protected either by an independent audit trail or by county and state tabulators which can prevent fraudulent manipulation. The court held:

> The use of touch screen voting systems is not subject to strict scrutiny simply because this particular balloting system may make the possibility of some kinds of fraud more difficult to detect. Rather, the question is whether using a system that brings about numerous positive changes, but lacks a voter verified paper ballot, constitutes a severe restriction on the right to vote. We cannot say that use of paperless, touch screen voting systems severely restricts the right to vote. No balloting system is perfect. Traditional paper ballots, as became evident during the 2000 presidential election, are prone to over-votes, under-votes and 'hanging chads' and other mechanical and human errors that may thwart voter intent. Meanwhile, touch screen voting systems remedy a number of these problems, albeit at the hypothetical price of vulnerability to certain types of fraud. The DRE voting system does not leave voters without any protection from fraud, or any means of verifying votes, or any way to audit or recount. The unfortunate reality is that the possibility of electoral fraud can never be completely eliminated no matter which type of ballot is used. Even assuming that none of the advantages of touch screen systems over traditional methods would be sacrificed if voter verified paper ballots were added to touch screen systems, it is the job of democratically elected representatives to weigh the pros and cons of various balloting systems. So long as their choice is reasonable and neutral, it is free from judicial second guessing. In this instance, Georgia made a reasonable, politically neutral and non-discriminatory choice to certify touch screen systems as an alternative to paper ballots. Nothing in the Constitution forbids this choice.
>
> [Favorito, supra, 684 S.E. 2d at 260-61, quoting Weber, supra 437 F.3d at 1106-1107 (11)(B). See also Mills, supra, 218 S.W. 3d at 33, 41-42.]

In Georgia, as in many states, voters have the option of casting an absentee ballot or using the touch screen election voting machines. Since every voter has the right to vote either by absentee ballot or by utilizing the DRE, the court rejected the notion that electronic voters are treated differently from voters who cast absentee ballots on paper or that there is some State based classification between voters. Finally, the court held that even assuming that such a classification of persons was involved, there clearly was no

suspect class and, unless a fundamental right is being infringed, the parties challenging the classification are required to convince the court that the classification has no rational basis.

Addressing the difference between the recount procedures, an issue also raised in Gusciora, supra, 395 N.J.Super. at 422, the court noted:

> If touch screen voters are burdened at all, that burden is the mere possibility that their ballots will receive a different, and alleged inferior, type of review in the event of a recount. Such a burden, borne of a reasonable nondiscriminatory regulation, is not so substantial that strict scrutiny is appropriate. Thus, we review Georgia's recount procedures to determine if they are justified by the State's important regulatory interests. There are important reasons for employing different recount procedures according to the type of voting system. The difference between these procedures are necessary given the differences in the technologies themselves and the types of errors voters are likely to make in utilizing those technologies. Unlike a voter using an absentee paper ballot, a touch screen voter either chooses a candidate for a particular race or does not; the touch screen machines do not record ambiguous indicia of voter intent that can later be reviewed during a recount. Accordingly, we hold that Georgia's recount procedures are justified by the State's important regulatory interest and, therefore, they do not violate equal protection.
>
> [Favorito, supra, 684 S.E.2d at 261-62, quoting Anderson, supra, 452 F.3d at 1232-1233 (111)].

In a recent decision, the United State Supreme Court recently denied certiorari of an unpublished opinion of the Fifth Circuit holding that a Texas United States District Court properly applied the deferential analysis of Anderson and Burdick in rejecting a claim that the use of a DRE without VVPATs impermissibly burdened the right to vote under the Due Process and Equal Protection Clauses of the United States Constitution. Tex. Democratic Party v. Williams, 285 Fed. Appx. 194, 195 (5th Cir. Tex. 2008), cert. denied, 2009 U.S. LEXIS 475 (2009). See Tex. Democratic Party v. Williams, No. A-07-CA-115-SS (W.D. Tex. August 16, 2007).

Clearly, no right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. This right has been clarified to mean, in essence, "the right to participate in an electoral process that is necessarily structured to maintain the integrity of the democratic system." Burdick, supra, 504 U.S. at 433. Subsumed within this right is

the power of the state to regulate elections to ensure orderly, rather than chaotic, operation of the democratic process. Storer v. Brown, 415 U.S. 724, 730, 94 S.Ct. 1274, 39 L.Ed. 2d 714 (1974).

In addition, beyond the standard to be applied in addressing the constitutional issues; to wit, a paperless versus paper system, this case also presents the issue of the scientific reliability of the voting system used in this State. Here, unlike many cases that address novel issues of scientific reliability of new devices, the DRE has been in use for twenty years and the State has a comprehensive legislatively-defined process for the review and certification of voting machines. State v Chun, supra, 194 N.J. at 54; Romano v. Kimmelman, 96 N.J. 66 (1984). Title 19, more specifically, N.J.S.A. 19:48-1 and N.J.S.A. 19:53, outlines the statutory factors that must be met to certify voting systems. While the statute provides that a certified voting system is entitled to a conclusive presumption, this court has already held a rebuttable presumption applies.

In this case, the court finds that the voting rights are not severely restricted by the use of paperless voting machines. First, the court finds that, absent pre-meditated criminal activity, the voting systems in this State are safe, accurate and reliable. In the case at bar, Appel and his team examined the AVC under artificial laboratory conditions with unfettered access to two AVC machines and the source code, for a period of one month. Second, there is no evidence of tampering of an AVC in any election in this State, or any impermissible alteration of any vote. Instead, the record is replete with testimony from State and County election officials that, over the many years of use, not one election result in the State has been adversely affected.[96] As a result, the heightened scrutiny test does not apply.

Further, in this case, as in Favorito, the use of touch screen voting systems is not subject to strict scrutiny simply because "this particular balloting system may make the possibility of some kinds of fraud more difficult to detect." Favorito, supra, 684 S.E. 2d at 260. As a result, the court is left with the issue of whether the challenged system imposes only reasonable nondiscriminatory restrictions on voting rights.

[96] The option switch bug has been remedied. The redundant memory capabilities of the AVC disclosed the error. The error was insufficient to have changed the results of the election.

If so, a minimal scrutiny test applies and the state's important regulatory interests are generally sufficient to justify the restrictions. Applying that standard, the State easily meets this test.

The court is satisfied that the State's decision to certify paperless DRE voting systems as an alternative to paper ballots, and the decision by the various counties to use such a system, represents reasonable nondiscriminatory choices, and thus do not violate a voter's equal protection or due process rights. The same result has been reached in other jurisdictions. Plaintiffs have not overcome the presumption in demonstrating that there are no conceivable grounds to support Title 19's validity; therefore, "it is the job of democratically-elected representatives to weigh the pros and cons of various balloting systems." Weber, supra, 347 F.3d at 1107.

Finding no constitutional impediment to the election process, it is well settled law that the separation of power is a fundamental principle of our State government. Article III, paragraph 1 of the New Jersey Constitution reads:

> The powers of the government shall be divided among three distinct branches, the legislative, executive and judicial. No person or persons belonging to or constituting one branch shall exercise any of the powers properly belonging to either of the others except as expressly provided in this Constitution.
>
> [Ibid.]

The Article establishing the separation of powers first appeared in its present form in the New Jersey Constitution of 1844. It was designed to "maintain the balance between the three branches of government, preserve their respective independence and integrity, and prevent the concentration of unchecked power in the hands of any one branch." David v. Vesta Co., 45 N.J. 301, 326 (1965)(footnote and emphasis omitted). This is an explicit constitutional mandate that "contemplates that each branch of government will exercise fully its own powers without transgressing upon powers rightfully belonging to a cognate branch." Knight v. Margate, 86 N.J. 374, 388 (1981).

Article II of the New Jersey Constitution, which is captioned "Elections and Suffrage," references the power of the legislative branch of government to enact laws regulating the electoral process. See

Gangemi, supra, 25 N.J. at 11. It is axiomatic that the right to vote is fundamental, as it is preservative of all other rights. See, e.g., Yick Wo, supra, 118 U.S. at 370. Paralleling this core democratic principle is the recognition "that states are entitled to broad leeway in enacting reasonable, even-handed legislation to ensure that elections are carried out in a fair and orderly manner." Weber, supra, 347 F.3d at 1105 (citing Storer, supra, 415 U.S. at 730 (1974) (noting "as a practical matter, there must be a substantial regulation of elections if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic process.")); Celebrezze, supra, 460 U.S. at 788 (recognizing that "there must be a substantial regulation of elections if they are to be fair and honest," and that states have broad leeway in "enact[ing] comprehensive and sometimes complex election codes ... [that] govern[] ... the voting process itself.").

Fundamental to any electoral infrastructure is the mechanism that collects and stores voters' ballot choices. The choice and the requirements of such a mechanism, originally conceived as the ballot box and now commonly known as the voting machine, is properly a legislative determination. By way of the Election Laws of New Jersey, Title 19, the Legislature has enunciated the standards that must be met by voting systems prior to their use within the counties. These standards are set forth in N.J.S.A. 19:48-1(a) through (n), and N.J.S.A. 19:53A-3 (a) through (h). These provisions ensure privacy to voters casting their ballots and enumerate specific safeguards that address the accurate recording and tabulation of votes. Additionally, Title 19 mandates the availability of emergency ballots, and provides that voting systems be designed and constructed such that they may be used "safely, efficiently, and accurately in the conduct of elections and counting ballots." N.J.S.A. 19:53A-3(g).

In this State, the Legislature has adopted strict requirements for voting machines. Subject to certain requirements, N.J.S.A. 19:48-1 provides that any thoroughly tested and reliable voting machines may be adopted, rented, purchased or used. Furthermore, a voting machine must first be certified before it may be used in any election in New Jersey. N.J.S.A. 19:48-2 and N.J.S.A. 19:53A-4 (electronic voting systems). N.J.S.A. 19:48-2 sets forth the procedure for the examination necessary for a voting machine to

be certified. The statute provides for a three-member Committee to consist of a patent attorney and two mechanical experts to examine the machine.

The role of the Legislature in structuring the State's electoral process has been long recognized by the courts. Over forty years ago, the Appellate Division held that:

> The process of public elections in this country is not of common law origin. Except for the express requirements of the constitutional security they are the creatures of statutory law. Therefore the courts refrain from an indulgence in any judicial action that refashions legislation regulating and facilitating the conduct of elections and which is calculated to secure the right of suffrage and the free expression of choice of the voter.
>
> [Sharrock v. Keansburg, 15 N.J. Super. 11, 16 (App. Div. 1951).]

As noted heretofore, in Weber, the district court found no evidence that the use of the county's voting system constituted differential treatment of voters, and concluded that plaintiff's right to vote had not been impaired. Supra, 347 F.3d at 1103. The AVC Edge system was a reasonable choice for a voting system that protected against fraud and advanced a number of important state interests. Ibid. Most importantly, the Weber court held that "it is the job of democratically-elected representatives to weigh the pros and cons of various balloting systems. So long as their choice is reasonable and neutral, it is free from judicial second guessing." Id. at 1107.

The Weber court's opinion was cited with approval more recently in Lapore, supra, 878 So.2d at 1276. In Lapore, The Court reiterated the corollary principles that while the right to vote is a fundamental right, there exists no guarantee of a perfect voting system. Id. at 1282.

The court notes that even if it were to analyze this case against a strict scrutiny standard under Greenberg, supra, 99 N.J. at 552, as urged by plaintiffs, the defendants still pass this test, as any interference with voters' rights in this State is an indirect, and not a substantial or intentional consequence of the use of the AVC system. First, the AVC provides voter verification and the ability to conduct recounts. N.J.S.A. 19:28-1. Second, and even more important, the use of the AVC has not impaired any individual's fundamental voting rights, as there has been no evidence presented that absent criminal conduct, any individual's vote was not counted.

G.

TITLE 19 COMMITTEE

Like all administrative decisions, the State argues that the 1987 certification of the AVC voting machines is entitled to a presumption of validity, with the burden on the party challenging the decision to demonstrate that it is arbitrary, capricious, unduly onerous, or otherwise unreasonable. The Supreme Court of New Jersey has repeatedly held that administrative agency decisions are entitled to a presumption of correctness and that the burden is on the party challenging the agency action to overcome this presumption. In re Musick, 143 N.J. 206, 216 (1996); In re March 24, 1992 Order, 132 N.J. 209, 221 (1993); Hills Dev. Co. v. Twp. of Bernards, 103 N.J. 1, 45 (1986); Dougherty v. Dep't of Human Servs., 91 N.J. 1, 6 (1982); N.J. Guild of Hearing Aid Dispensers v. Long, 75 N.J. 544 (1978). The Appellate Division has faithfully applied these principles. As that court recently explained, "[t]here is a strong presumption that an agency decision is valid. One challenging that decision has a heavy burden of proving the contrary and demonstrating that the decision was arbitrary, unreasonable or capricious." In re Tax Credit of Pennrose, 346 N.J. Super. 479, 486 (App. Div. 2002); Coalition for Quality Health Care v. Dep't of Banking & Ins., 348 N.J. Super. 272, 301 (App. Div.), certif. denied, 174 N.J. 194 (2002).

The State also argues that the Secretary of State's determination that recertification was not required is entitled to substantial deference. See R&R Mktg., L.L.C. v. Brown-Forman Corp., 158 N.J. 170, 175 (1999). While courts generally give substantial deference to the interpretation an agency gives to a statute that the agency is charged with enforcing, in this case, the court finds it inapplicable. First, the court finds that the present composition of the Title 19 Committee, and most likely the composition in the past, failed to meet the requirement that two of the members be "mechanical experts." Second, based on the number of modifications made to the AVC, a full review of the AVC is required.

N.J.S.A. 19:48-2, entitled "Examination of Voting Machines by Secretary of State," provides that "any person or corporation owning or being interested in any voting machine may apply to the Secretary of State to examine such machine." The statute requires the Secretary of State to examine the machine

within thirty days and to make and file in their office a report of the examination. If approved, the machine(s) may be used at elections.

The statute, in pertinent part, also provides that:

> Before making such report the Secretary of State shall require the voting machine to be examined by three examiners to be appointed for such purpose by him, one of whom shall be an expert in patent law and the other two mechanical experts, and shall require of them a written report on such machine, which the Secretary of State shall attach to his own report on the machine.
>
> [N.J.S.A. 19:48-2.]

N.J.S.A. 19:48-2, adopted in 1953, L. 1953, c. 302, § 2, did not require members of the committee to possess any computer knowledge or skill. That is certainly understandable, as noted by plaintiffs, given the fact that the committee was created in 1953. At the time the statute was enacted, the court assumes lever or other mechanical voting systems were in place.

The term "mechanical" is defined as "pertaining to the design, use, understandings, etc., of tools and machinery." www.dictonary.com. The term "expert" is defined as "a person who has special skill or knowledge in some particular field." www.dictionary.com. Today, all twenty-one counties use electronic voting machines, a computer-based voting machine system. This type of voting system is significantly different than the former mechanical machines. As a result, the term "mechanical expert" should be construed to mean a person who understands and has experience and training in modern day electronic voting machines to evaluate and address the complexities of the internal and external operation of a modern day, computer-based voting system.

While Woodbridge meets the requirement that one of the members of the Committee shall be a patent attorney, whether Mahoney and/or Fleming meet the "mechanical expert" requirement is more difficult. The court will consider each member separately.

Mahoney, a high school graduate, has been a member of the Title 19 Committee for six years. With some vocational training in auto mechanics, Mahoney was hired in 1993 as a mechanic to clean, repair, and reset voting machines. Mahoney is currently the Assistant Director of Voting Machines and

oversees the operation of the warehouse. Mahoney has never taken any computer courses or received computer training in any past or current positions, and is not familiar with computer programming languages, engineering or security-related courses. During the trial, Mahoney testified that in resolving computer related issues, he relied on Committee member Fleming and the vendors.

In response to questions on cross-examination, Mahoney testified that the Committee does not examine source code, rely on the advice of computer scientists or security experts, or conduct independent research. While Mahoney has repaired voting machines and is familiar with election administration, his background and experience do not satisfy the statutory requirement of a "mechanical expert."

Fleming, a member of the Committee since 2001, holds a Bachelor's degree in Psychology from Trenton State College. Before working for the State, Fleming worked as an x-ray technician. Currently employed by the Attorney General's Office, he has no formal education in computer science, computer programming, or computer security. For the past twenty years, however, he has taken approximately twenty to thirty courses on a wide range of different operating systems. He does not write computer programs and does not understand the "C" language of the AVC 9.00H.

Fleming is in charge of the computer systems at the Attorney General's Office. In this position, he installs software, maintains the servers, networks, wiring, switches and routers, and replaces parts. Clearly, Fleming is knowledgeable about computer operating systems and appears more than capable of maintaining same. The critical question is whether or not this is sufficient to meet the definition of "mechanical expert." In the highly technical and sophisticated computer community that we live in today, the court finds that the term "mechanical expert" means an individual that has a basic understanding of, not only computer operating systems, software installation, and repairs, but also a fundamental understanding of software and hardware architecture.

The members of the Committee testified that they do not consult with independent experts or conduct any type of research as part of their examination. While this would be understandable if two of the members were "mechanical experts" it is particularly troubling in this case. Here, neither Mahoney

nor Fleming qualify as mechanical experts, and rely, to a great extent, on the materials and presentation of the vendors.

In this State, all twenty-one counties rely on computer-based voting machines. For some period of time, during this litigation, at the suggestion by the court that the State secure the services of a third party professional to intervene in the review process, the New Jersey Institute of Technology became involved. The court is not aware of the current status of that involvement.

Suffice it to say, the Secretary of State should take immediate steps to nominate two "mechanical experts" consistent with the definition articulated by the court, to the Title 19 Committee, in order to meet the requirements of the current statute. In the alternative, the State may find it appropriate to consider legislation to amend the statute to include the appointment of an academic institution as a member of the Committee or to rewrite the statute in some alternative way to meet the challenges and issues for all of the voting machines used today that utilize systems based on computer hardware and software.[97] That decision is one for the Secretary of State and Legislature, and not the court.

The determination that the Title 19 Committee must be reconstituted raises several issues. The first, and most important, is what action the court should undertake in the interim. The second is the time to be afforded the State to appoint two new members to the Title 19 Committee or adopt legislation to change the method in which voting machines are tested. Clearly, as will be outlined herein, the court will be making recommendations beyond the composition of the Title 19 Committee.

Based on the court's review of the entire record, the court is satisfied that, in the interim, the wise and prudent decision is for the State to continue to use the AVC. First, in 1994, the AVC was successfully tested to the 1990 VSS and has been successfully used for over fifteen years in hundreds of municipal, county and state elections. Moreover, to ensure its accuracy and reliability, several testing procedures are required before an AVC voting machine is used in an election. This includes maintenance diagnostic procedures, set-up diagnostic procedures and Pre-LAT testing. For purposes of this record, it is noted that

[97] As noted by all of the experts, however, it is also important for at least one member to understand or be familiar with election administration.

no vote count has been changed as a result of a recheck nor has any election been overturned due to a machine malfunction.

The newly constituted Title 19 Committee shall, within 120 days from today, issue a report to the Secretary of State as to whether to recommend continued use of the AVC in this State. The court directs the Title 19 Committee to conduct a full certification examination of the AVC as currently configured.[98]

The Secretary of State shall have 60 days from the receipt of the report from the newly constituted Title 19 Committee to make a final decision.

V.

SPECIFIC REQUIEMENTS OR RECOMMENDATIONS

1. HARDENING GUIDELINES ANTI-VIRUS SOFTWARE (REQUIRED)

Chapter Eight of the Sequoia Voting Systems, Election Management System Manual, entitled "Additional Security Guidelines," dated March 5, 2008, identifies steps to take to ensure an election tabulation environment as free from outside contamination as possible. It specifically recommends that certain steps be taken.

This document is under seal. Therefore, the court will not disclose the specific recommendations. Based on the testimony adduced at trial, Sequoia recommends customers to install both hardening and anti-virus applications.[99] Additionally, customers are advised that laptops not be connected to the Internet or be used for any other purpose. The record reflects that New Jersey has not adopted any of the hardening guidelines and that anti-virus software, if installed, is done so sporadically.

According to Sequoia, hardening techniques and anti-virus software are available at little or no cost to the State.[100] This shall be completed on or before the 120 days set forth in the prior section.

---

[98] While the AVC was originally approved in 1987, in 1994 an independent ITA verified that the AVC met the 1990 standards. Therefore, in considering the AVC, the Title 19 Committee shall conduct a complete recertification to ensure that, as presently configured the AVC meets the statutory criteria set forth herein.

[99] The State's experts also recommend implementation of hardening and antivirus measures.

[100] The court also recommends that the results cartridges be encrypted in future systems.

2. BACKGROUND CHECKS (RECOMMENDED)

The integrity of our voting system depends on a system designed to protect voting machines against attack by intruders. During the trial, Clayton, Giles, Mahoney and Gentile described the manner in which voting machines are stored in the warehouse. The voting machine warehouses are located separate and apart from county administration offices in buildings that are either owned or rented by the county.

Without exception, the premises are locked and each employee utilizes a code to enter the building and/or activate or deactivate the alarm. During the evening and on the weekends, the buildings do not have security personnel on site. While these rudimentary security measures are most likely adequate to preclude entry from an outside intruder, the most likely attack will occur through the actions of an employee, contract vendor, or consultant.

None of the witnesses were aware of any policy that required warehouse employees, contract vendors, or consultants to undergo criminal or security background checks. Given the importance of ensuring the safety and security of voting machines, election officials should require all new employees, vendors, and consultants to be subject to criminal background investigations. While this will not necessarily prevent an attack in all circumstances, requiring a criminal background check will help to protect the integrity of the process. As noted in the trial record, some of the counties utilize outside vendors or consultants to conduct Pre-LAT, upgrade software, installations, maintenance, or other tests. While performing these tasks, these individuals are oftentimes given unsupervised access. Clearly, election officials should require employees, vendors or consultants with access to voting machines to be subject to criminal and security background checks. Additionally, access by outside consultants and vendors should be done under strict supervision and control.

3. TRANSPORTATION/DELIVERY/RETURN OF VOTING MACHINES (RECOMMENDED)

The record reflects that in New Jersey, and many other states, voting machines are left unattended for weeks before the election and weeks after the election. The risk is not unique to the AVC voting

system. This schedule results from the large number of polling places and the number of voting machines to be delivered to polling places.

Warehouse election representatives testified that voting machines are transported to polling places by third party vendors hired by the county. But for one of these counties, warehouse election personnel do not accompany the movers during the transportation and delivery of the machines. Furthermore, once the machines are delivered to the polling place, the warehouse is not advised by the movers or representatives from the polling places that the machines have been delivered.

According to warehouse representatives, delivery of voting machines to the polling places begins as early as two weeks before the election. The testimony and photographs produced by Felton disclosed polling places left open during the day and sometimes into the evening. There are no security cameras and there are often signs that direct individuals to the place of the voting machines. As confirmed by Felton, an intruder can go undetected for long periods of time and have unrestricted access to the machines.

Since voting machines are left unattended in public places for several days, sometimes weeks, before and after each election, it is not difficult to gain unsupervised access to the voting machines. After the election, the voting machines remain at the polling places for up to two weeks before being returned to the warehouse. Importantly, there are no written or unwritten policies or protocols in place that govern the storage, transportation, or return of the voting machines to the warehouse.

While the court understands the difficulty in delivering the voting machines on the day of the election, voting machines should not be left in unsecured areas. Even though tamper-evident seals help remediate the risk associated with leaving voting machines unguarded, leaving machines unattended for several weeks is problematic. Still, having both these locks and seals means the intruder must know how to pick a lock without breaking it, and know how to break and replace a seal without leaving detectable evidence. Tamper-evident seals also generally have serial numbers on them, requiring the intruder to replace the seals with ones that have the identical numbers.

Based on this information, the court directs the State, County, and Municipal election representatives to undertake an examination of the current procedures and make recommendations to

guard against potential voting machine tampering. One recommendation is that security cameras be required for any facility where voting machines are left prior to and after an election. The cost of these devices in today's market should be minimal. A cost-benefit analysis clearly weighs in favor of this kind of security equipment.

4. SEALS AND SEAL-USE PROTOCOLS (REQUIRED)

For a system of tamper-evident seals to provide effective protection seals must be consistently installed, they must be truly tamper-evident, and they must be consistently inspected. While the new seals proposed by the State will provide enhanced security and protection against intruders, it is critical for the State to develop a seal protocol, in writing, and to provide appropriate training for individuals charged with seal inspection. Without a seal-use protocol, use of tamper-evident seals significantly reduces their effectiveness.

The court directs the State to develop a seal-use protocol. This shall include a training curriculum and standardized procedures for the recording of serial numbers and maintenance of appropriate serial number records.

5. INTERNET CONNECTION AND OTHER TRANSMISSION LINES (REQUIRED)

As long as computers, dedicated to handling election matters, are connected to the Internet, the safety and security of our voting systems are in jeopardy. Therefore, if the State has not done so already, Clerks shall be advised that computers utilized for election-related duties shall <u>at no time</u> be connected to the Internet. (emphasis added.)

Each Clerk shall conduct an examination of the means in which election data is transmitted to the Clerk after an election. Once the information is collected, the State shall assist the counties in developing action plans to ensure the integrity of the transmittal of voting data between the Municipal Clerks' offices and the Clerk. If counties do not provide a plan, then and in that event, results cartridges shall be personally delivered to the Clerk for tabulation.

6. TRAINING AND RECORD-KEEPING (RECOMMENDED)

It is imperative for the State to develop and implement Statewide training and training materials for Clerks, Boards, Superintendents, technicians, warehouse personnel and poll workers. Part of that training must include protocols for the chain of custody and maintenance of election records and documentation, including, but not limited to, authorization slips, poll books, results cartridges, seals and serial numbers, emergency ballots, provisional ballots, mail-in, military and overseas ballots, ballot bags and machine tapes and printouts.

In addition, the Secretary of State should develop auditing criteria to verify election results and to ensure adherence to protocols in all municipal, county, state and federal elections.

VI.

CONCLUSION

Counsel for the State shall prepare an order consistent with this opinion. To ensure compliance with the items listed in the prior section, for a limited period of time, this court shall retain jurisdiction.