PENNY M. VENETIS, ESQ.
RUTGERS CONSTITUTIONAL LITIGATION CLINIC
123 Washington Street
Newark, New Jersey 07102
Tel: (973) 353-5687

JOHN McGAHREN, ESQ.
CAROLINE BARTLETT, ESQ.
PATTON BOGGS LLP
The Legal Center
One Riverfront Plaza, 6th Floor
Newark, New Jersey 07102
Tel: (973) 848-5600
Fax: (973) 848-5601
Attorneys for Plaintiffs

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. L-2691-04 CIVIL ACTION

PLAINTIFFS' UNREDACTED PROPOSED FINDINGS OF FACTS

This document was submitted to the trial court on July 3, 2009. It summarizes all of the evidence presented in the Plaintiffs' case. We firmly believe that it shows that New Jersey's paperless DREs can be hacked easily and made to steal votes. As such, the DREs violate both the NJ Constitution and Title 19 of the New Jersey Statutes.

This document was kept from the public (for over a year) by the Court, pursuant to a request by the New Jersey Attorney General's office. When finally ordered by the Court to justify, legally, on a line-by-line basis, why this document should be kept secret, the Attorney General's office instantly capitulated. The Attorney General's office failed to articulate a single reason why this document should be kept from the public. The Court subsequently signed an order on October 15, 2010 permitting us to release the entire document to the public.

You may notice that some portions of this document are redacted. Our expert witness, Dr. Roger Johnston, advised us to remove sections of the report concerning his methodology for defeating certain security seals contemplated for use by the State. The removal of this information from the report does not in any way detract from Dr. Johnston's clear conclusions—that the locks and seals contemplated for use by the State of New Jersey do not secure the State's voting machines.

TABLE OF CONTENTS

I. Testimony of Plaintiff Stephanie Harris

1. Plaintiff, Stephanie Harris, is a twenty-five-year resident of Hopewell, New Jersey. (Testimony of Stephanie Harris ("Harris Test."), Jan. 27, 2009 Trial Tr. at 70:9-13.)

2. Ms. Harris has a Bachelor of Science degree from Brandeis University and a Master of Arts and Teaching from Harvard University. (Id. at 70:23-24.)

3. Ms. Harris is a registered New Jersey voter and she votes in New Jersey elections. (Id. at 71:3-8.)

4. The voting machines used in Mercer County where Ms. Harris is a registered voter are Sequoia AVC Advantage 9.00H Direct Recording Electronic ("DRE") machines.

5. Shortly before the first time Ms. Harris was to vote on the Sequoia DRE in the June 2004 Presidential primary election, Ms. Harris attended a demonstration of those DREs and a training class on how to use them. (Id. at 71:22 to 72:8.) During the training class, she received written instructions on how to use the DRE and had an opportunity to cast a mock vote. (Id. at 72:11-14.)

6. On June 8, 2004, Stephanie Harris went to the Hopewell Elementary School to vote in the Presidential primary election. (Id. at 72:15 to 73:1.) It was the first time Ms. Harris voted on a Sequoia AVC Advantage DRE. (Id. at 71:13-21.) She entered the voting booth and pressed the buttons next to the names of the candidates for whom she wished to vote. Then, she pressed the "cast vote" button, and exited the voting booth. (Id. at 73:1-4.)

7. Immediately after exiting the voting booth, Ms. Harris was informed by a poll worker that her vote was not counted. (Id. at 73:10-12.) She was instructed to re-enter the voting booth and press the "cast vote" button a second time. (Id.)

8. Upon exiting the voting booth a second time, Ms. Harris was again informed that her vote was not counted. (Id. at 73:12-14.)

9. For a third time, Ms. Harris was instructed to return to the voting booth and press the "cast vote" button. (Id. at 73:13-15.) Again, the poll worker told Ms. Harris that her vote was not counted. (Id. at 73:14-17.)

10. After a fourth attempt to cast her vote, the poll worker told Ms. Harris that he thought the voting machine registered her vote. (Id. at 73:16-18.) Neither the poll worker nor Ms. Harris could be sure that her vote was actually counted. (See Id.)

11. The poll worker was present outside the voting booth each of the four times Ms. Harris attempted to cast her vote, but never offered Ms. Harris an emergency ballot as an alternative method of casting her vote. (Id. at 73:19-24.)

12. In order to protect her right to vote and to ensure that her vote is always accurately cast and counted, Ms. Harris has voted by absentee ballot in all elections but one since June 8, 2004. (Id. at 74:3-7.)

13. Since 2004, Ms. Harris has worked with the State Legislature as well as the United States Congress to get voter verification bills and audit bills passed to ensure that her own votes and the votes of others are accurately counted. (Id. at 74:8-17.)

14. Ms. Harris also filed this lawsuit to ensure that her vote is counted. (Id.)

II. Testimony of Plaintiffs' Expert Witness Professor Andrew Appel

A. Professor Appel is an Extraordinarily Qualified Witness in the Fields of Computer Science, Computer Security, the Sequoia Advantage DRE and the WinEDS System

15. Professor Appel has been a professor of computer science at Princeton University since 1986, tenured since 1992, and a full professor at Princeton since 1995. (Testimony of Andrew Appel ("Appel Test."), Jan. 27, 2009 Trial Tr. at 80:22 to 81:3.)

16. Professor Appel received a Bachelor's degree in Physics with highest honors from Princeton in 1981. (Appel Test., 1/27 Trial Tr. at 82:14-23.) He also received, at graduation, the Kusaka Memorial Prize in Physics, an award for excellence in undergraduate senior thesis research. (Appel Test., 1/27 Trial Tr. at 82:19-83:3.) A specialty in his undergraduate work was applications of computer science to Z80 chips applying computers to medicine. (Appel Test., 1/27 Trial Tr. at 83:16 to 84:1.) Professor Appel has been doing research in computer science since 1980, and researching computer security since 1994. (Appel Test., 1/27 Trial Tr. at 93:20-24.)

17. Professor Appel earned a Ph.D. in Computer Science from Carnegie Mellon University in 1985. (Appel Test., 1/27 Trial Tr. at 84:2-11.) His main areas of Ph.D. research were programming languages, compilers, and formal methods (Appel Test., 1/27 Trial Tr. at 84:13-14), which are methods of reasoning about computer software to ensure that it is correct and accurate. (Appel Test., 1/27 Trial Tr. at 84:15-16.) His dissertation was about semantics-directed compilers. (Appel Test., 1/27 Trial Tr. at 84:19-20.) During his graduate work, he earned a

National Science Foundation fellowship, a merit-based fellowship awarded only to a small number of the many applicants. (Appel Test., 1/27 Trial Tr. at 84:21 to 85:5.)

18. Professor Appel's employment during his graduate work included: teaching and research assistantships, summer jobs at a financial forecasting software company in New York, and a research position at Bell Laboratories in Murray Hill, New Jersey. (Appel Test., 1/27 Trial Tr. at 85:6-14.) His affiliation with Bell Laboratories continued after he received his Ph.D., and from 1983 until twenty years later, he regularly served as a computer science consultant at Bell Laboratories. (Appel Test., 1/27 Trial Tr. at 85:15-20.) This consulting work involved programming languages, compiling, and formal methods. (Appel Test., 1/27 Trial Tr. at 85:21-24.)

19. Professor Appel also has an appointment to an interdisciplinary center at Princeton University called the Center for Information Technology Policy, which studies the intersection between computer science and public policy, brings together researchers from both these fields to interact, and to analyze how technology can be useful in public policy and vice versa. (Appel Test., 1/27 Trial Tr. at 86:14-25.) The Center is a joint venture between the Engineering School at Princeton University and the Woodrow Wilson School of Public and International Affairs, also at Princeton University. (Appel Test., 1/27 Trial Tr. at 87:1-6.)

20. Professor Appel was Associate Chair of the Department of Computer Science at Princeton University for about ten years between 1996 and 2005, and will become

the next Chair of the Computer Science Department at Princeton University. (Appel Test., 1/27 Trial Tr. at 87:12-21.)

21. Professor Appel teaches courses at Princeton in software engineering, programming languages, compilers, election machinery, and other topics. (Appel Test., 1/27 Trial Tr. at 87:22-25.) Professor Appel's course on election machinery involves not only voting machines, but also political party machines, and the machinery of election administration by public officials. (Appel Test., 1/27 Trial Tr. at 88:1-5.)

22. Professor Appel has been a Fellow in the Association for Computing Machinery since 1998. (Appel Test., 1/27 Trial Tr. at 92:3-5.) The Association for Computing Machinery is an international professional society of computer scientists, both in academia and industry, with tens of thousands of members. (Appel Test., 1/27 Trial Tr. at 92:7-13.) The Association for Computing Machinery honors approximately forty members a year, for excellence in research and service accomplishments, by designating them as Fellows of the Association. (Appel Test., 1/27 Trial Tr. at 92:14-19.)

23. Professor Appel has continuously received research grants for his professional work since he began his career in 1986. (Appel Test., 1/27 Trial Tr. at 92:24 to 93:2.) One of the more notable grantors is the National Science Foundation, for Professor Appel's research in programming languages, compilers, and computer security. (Appel Test., 1/27 Trial Tr. at 93:3-8.) Additionally, he has received research grants from the Defense Advanced Research Projects Agency for research in computer security, and from the Advanced Research and Development

Activity, a funding agency within the United States Intelligence Community. (Appel Test., 1/27 Trial Tr. at 93:8-12.) He recently received a grant for research in computer security from the United States Air Force Office of Scientific Research. (Appel Test., 1/27 Trial Tr. at 93:13-16.) In addition to research grants from government agencies, Professor Appel has also received research grants from many corporations, such as IBM, Microsoft, and Sun Microsystems. (Appel Test., 1/27 Trial Tr. at 93:17-19.)

24. Professor Appel teaches computer security in the context of software engineering courses at the sophomore level, but he also advises research graduate students who do computer security research. (Appel Test., 1/27 Trial Tr. at 88:6-13.) This entails suggesting research topics to the graduate students, participating with them in that research, co-authoring scientific papers with his students on computer security, sitting on oral examination committees of his own graduate students and other graduate students, and other supervisory tasks. (Appel Test., 1/27 Trial Tr. at 88:14:23.)

25. Professor Appel does extensive scientific research, ranging from theoretical aspects of computer security that overlap with programming languages and formal methods, to practical computer security topics, such as securing enterprise computer networks, physical security, and security of computer memory systems, among others. (Appel Test., 1/27 Trial Tr. at 89:1-9.)

26. Professor Appel's curriculum vitae enumerates ninety publications, of which eighty-three, including two books and a chapter of another book, were published in peer reviewed venues. (Appel Test., 1/27 Trial Tr. at 94:4-24.) The books are

mostly about compilers, which are the computer programs that translate human-readable source code (which programmers write) into machine-readable source code (which computers run). (Appel Test., 1/27 Trial Tr. at 95:2-4.) The chapter that he wrote for a third book concerns "garbage collection," a term of art for managing computer memory by reclaiming space that is occupied by data that is no longer needed, so that it can be used again. (Appel Test., 1/27 Trial Tr. at 95:5-11.)

27. Professor Appel has been an associate editor of two journals. (Appel Test., 1/27 Trial Tr. at 95:17-19.) He also served as editor-in-chief for the Association for Computing Machinery's journal, TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS, for about four-and-a-half years. (Appel Test., 1/27 Trial Tr. at 95:15-21.) Additionally, he was co-editor of some issues of other journals, including the JOURNAL OF FUNCTIONAL PROGRAMMING. (Appel Test., 1/27 Trial Tr. at 95:22 to 96:1.) During the course of his editorial career at the Association for Computing Machinery's Journal, TRANSACTIONS ON PROGRAMMING LANGUAGES AND SYSTEMS, he supervised hundreds of papers through the publication process, from submission to publication. (Appel Test., 1/27 Trial Tr. at 96:13-17.) These included papers on computer security. (Appel Test., 1/27 Trial Tr. at 96:18-20.)

28. Professor Appel has also served as a member of the program committee, or a chair of the program committee, of several different conferences on computer science. (Appel Test., 1/27 Trial Tr. at 96:21 to 97:12.) A program committee for a scientific conference solicits presentations and the research papers which

accompany presentations on some particular subtopic in the scientific field. (Appel Test., 1/27 Trial Tr. at 96:25 to 97:4.) Subtopics of conferences for which Professor Appel has served on the program committee include programming languages, compilers, logic, voting machines, and other topics. (Appel Test., 1/27 Trial Tr. at 97:4-8.) Additionally, in 1992, he served as program chair for the Association for Computing Machinery's conference on principles of programming languages; meaning that he selected the members of the program committee. (Appel Test., 1/27 Trial Tr. at 97:9-20.) The program committee and the program chair jointly decide which papers to accept for publication and presentation, and run the process of soliciting papers. (Appel Test., 1/27 Trial Tr. at 97:14-20.)

B. Professor Appel has a Rock Solid Foundation for his Expert Opinion in this Case

29. In connection with this lawsuit, in July and August of 2008, Professor Appel and a team of computer scientists examined two Sequoia AVC Advantage 9.00H DREs provided by Defendants. (Expert Report of Andrew W. Appel ("Appel Report"), August 29, 2008, § 1.3, at 7; Appel Test., 1/27 Trial Tr. at 118:20-24.)

30. Professor Appel's team consisted of Professor Appel; Professor Brian W. Kernighan, another tenured computer science professor at Princeton who is one of the inventors of the "C Language," (the language in which the Sequoia Advantage 9.00H source code is written); Gang Tan, Assistant Professor of Computer Science at Boston College and Lehigh University; Maia Ginsburg, a lecturer in Computer Science at Princeton; Christopher D. Richards, a graduate student in Computer Science at Princeton; and Harri Hursti, an independent computer

security consultant and voting machine expert. (Appel Test., 1/27 Trial Tr. at 141:11-24; Appel Report, § 1.4, at 7 n.1.)

31. Professor Appel and his team spent an extraordinary number of man-hours inspecting and experimenting on the Sequoia AVC Advantage 9.00 DREs. His team spent almost seven days a week during the month of July 2008 examining the DREs, working between six to ten hours a day. (Appel Test., 1/27 Trial Tr. at 142:8 to 143:2.) Pursuant to Court order, the examination took place at a remote location a distance of one half-hour from Princeton. Gusciora v. Corzine, No. MER-L-2691-04 (Law Div. May 20, 2008) (Protective Order, ¶ 11, at 7.) The scientists could not bring their cell phones into the examination room, and had no Internet access. (Id.)

32. Even under these difficult examination constraints, the time window for examining the DREs was limited by this Court to thirty days. Gusciora v. Corzine, No. MER-L-2691-04 (Law Div. June 20, 2008) (Modified Protective Order, at 1.) The Defendants further erected numerous obstacles to Plaintiffs' examination, depriving Professor Appel and his team of the opportunity to perform some tests and procedures they would otherwise have conducted. Despite repeated promises to replace defective daughterboards after they ceased functioning, Defendants never did so, depriving Plaintiffs of an opportunity to demonstrate numerous flaws in these components. (Exs. P-22A, P-22B, P-22C, P-22D, P-22E.)

33. Further, despite having had months of time to prepare for the Court-ordered examination of the Sequoiua DREs, on June 30, 2008, Sequoia produced a grossly

incomplete subset of the source code, which failed to include the source code for numerous third-party library files, lacked build tools such as a compiler, and completely lacked any source code, firmware, or configuration files for the operating system on the daughterboard. (Appel Report, § 54.5-7 at 112-13.)

34. If given the time, Professor Appel would have fabricated a fraudulent Z80 chip. (Testimony of Andrew Appel ("Appel Test."), Jan. 28, 2009 Trial Tr. at 143:17-24.) This project would have taken Professor Appel at least a month, and possibly as long as three months. (Testimony of Andrew Appel ("Appel Test."), Jan. 29, 2009 Trial Tr. at 28:2-5.)

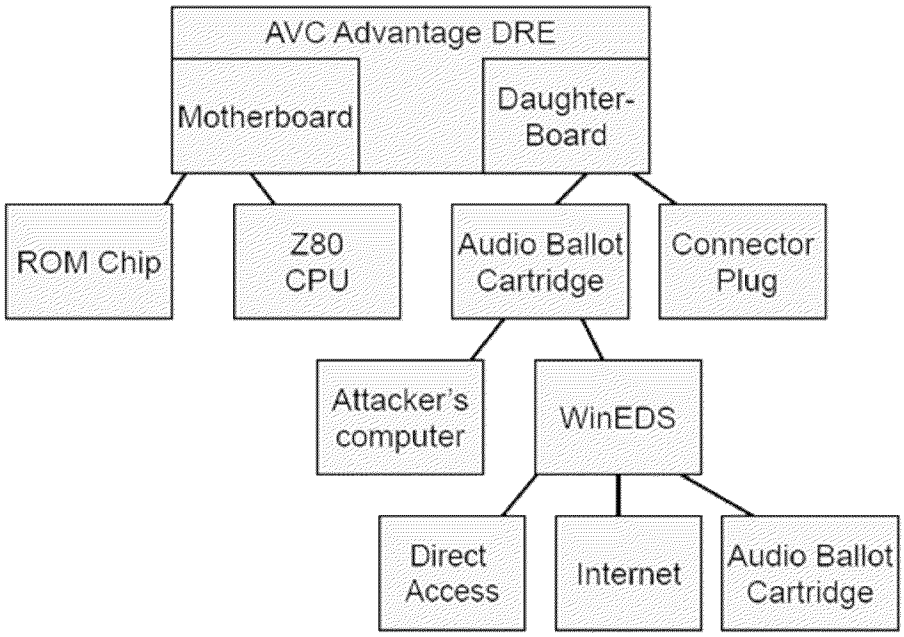
35. Despite these difficulties, Professor Appel and his team were able to examine the Sequoia Advantage 9.00H DREs long enough to conduct significant experimentation and to reach conclusions about the reliability, accuracy, and security of the Sequoia Advantage 9.00H. (Appel Test., 1/27 Trial Tr. at 143:3-6.)

36. Following the examination of the Sequoia 9.00H DREs, Professor Appel wrote a lengthy and detailed Expert Report containing narrative descriptions of all of the different insecurities and inaccuracies in the AVC Advantage DREs that he was able to uncover during the thirty-day examination. (Appel Test., 1/27 Trial Tr. at 143:18-23.) The Expert Report is not an exhaustive encyclopedia of all flaws and insecurities in the Sequoia Advantave DRE. (Testimony of Andrew Appel ("Appel Test."), Feb. 5, 2009 Trial Tr. at 11:11 to 12:8.) It discusses only flaws which could be uncovered and fully analyzed in a thirty-day period, parts of which were spent trying to obtain materials from Sequoia. (Id.) The flaws

Professor Appel uncovered, however, provide sufficient basis for his sound conclusions that the Sequoia Advantage 9.00H is unreliable, inaccurate, and insecure. (Appel Test., 2/5 Trial Tr. at 11:11 to 12:8; Appel Report, § 68, at 143-44.)

37. After thirty days of studying the Sequoia Advantage 9.00H DRE and its accompanying WinEDS system, Professor Appel found that the AVC Advantage could be attacked in all of the ways demonstrated by the chart below:

PATHWAYS TO INSERT FRAUDULENT FIRMWARE INTO THE AVC ADVANTAGE



39. As will be discussed in greater detail herein, the results of the attacks to the DRE and WinEDS system can be a complete, undetected stealing of votes or a complete disabling of targeted DREs.

40. The State of New Jersey did not put on any witnesses to testify that the Sequoia AVC Advantage DREs are secure and reliable. The Court precluded Dr. Shamos

from presenting an opinion as to the security or reliability of any part of any DREs used in New Jersey. (Appel Test., 1/27 Trial Tr. at 38:4-6.) Thus, Professor Appel's testimony on these matters was not contested by the State.

41. Professor Appel and his team examined a number of aspects of the Sequoia AVC Advantage 9.00H DREs, including but not limited to source code, the operation of the DREs, and how the WinEDS database computers interact with the DREs. (Appel Test., 1/27 Trial Tr. at 144:5-15.)

42. Additionally, on August 20 and 21, 2009, Professor Appel created a videotape demonstrating inaccuracies and insecurities of the Sequoia DREs. (Appel Test., 1/27 Trial Tr. at 147:22 to 148:-3.) Always present during the videotaping were one lawyer for the Plaintiffs, Ms. Venetis; at least one lawyer for the State, including Jason Postelnik, Donna Kelly, and Leslie Gore; and at least one lawyer representing Sequoia. (Appel Test., 1/27 Trial Tr. at 148:10-20.) The original videotapes were then converted into digital format and copied to three DVDs, which accompanied Professor Appel's Expert Report. (Appel Test., 1/27 Trial Tr. at 148:21 to 149:15.) Additionally, Professor Appel created a fourth DVD with selected material of particular relevance and importance. (Appel Test., 1/27 Trial Tr. at 149:11-18.) The videotape was transferred to four DVDs that were included in Professor Appel's Expert Report. (Exs. P-3, P-4, P-5, P-6.)

43. Professor Appel has worked on this case for nearly five years without compensation. (Appel Test., 2/5 Trial Tr. at 61:6-15.) He is working pro bono as a public service, because he views it as part of his role as a computer scientist and a professor in our society. (Appel Test., 2/5 Trial Tr. at 61:24-25.) He testified

that the role of a professor is not solely to conduct research, publish in scientific journals, and teach students, but is also to communicate to the broader public, to society, and to policymakers on research and findings within his expertise knowledge that are critical to formulating sound public policy. (Appel Test., 2/5 Trial Tr. at 61:16-25.)

44. The public service Professor Appel is performing by devoting his time to this lawsuit is ensuring the integrity of elections, one of the cornerstones of our democracy. (Appel Test., 2/5 Trial Tr. at 62:1-5.) Professor Appel is willing to take whatever time is necessary to communicate to the public and to this Court whatever expertise he has bearing on the integrity of elections. (Appel Test., 2/5 Trial Tr. at 62:5-8.)

45. Professor Appel has been certified by this Court as an expert in computer science and in computer security. (Appel Test., 1/27 Trial Tr. at 98:7-14.) This Court has also certified Professor Appel as an expert on the Sequoia AVC Advantage DRE that is the subject matter of this trial. (Appel Test., 1/27 Trial Tr. at 130:18-20.)

46. This Court also certified Professor Appel as an expert witness in 2006, where at trial, he was permitted to testify extensively about computer science and security issues related to DREs in general, including the Sequoia Advantage, and about the Z80 microprocessor.

47. Professor Appel's expertise in the field of computer security includes expertise in physical security. (Appel Test., 1/27 Trial Tr. at 89:3-9.) This component of computer security consists of physically securing machines containing computer components against tampering. (Appel Test., 1/27 Trial Tr. at 89:10-22.)

Securing the interior of a computer against attackers who seek to replace internal components of the computer is a critical aspect of the physical security component of computer security. (Appel Test., 1/27 Trial Tr. at 89:14-22.)

48. Threats to computer security can be conceptually divided into two types: (1) physical security where an attacker has physical access to the computer itself and can freely tamper with it, (Appel Test., 1/27 Trial Tr. at 91:7-13), and (2) the security of network systems, where someone can attack the computer without ever coming near. (Appel Test., 1/27 Trial Tr. at 89:23 to 90:11.)

49. Once attackers are prevented from physically accessing the machine, the next question for scientists studying computer security is whether the computer can be attacked over a network. (Appel Test., 1/27 Trial Tr. at 91:19 to 92:2.)

C. Description of the Sequoia Advantage 9.00H DRE

50. The Sequoia AVC Advantage 9.00H is a Direct Recording Electronic ("DRE") voting machine. (See Appel Test., 1/27 Trial Tr. at 106:20-25; Appel Report, § 2.1, at 9.)

51. A DRE is a computer with a user interface, such as a touch screen or a panel, which stores votes during an election and can communicate election results at the end of the day. (Appel Test., 1/27 Trial Tr. at 104:24 to 105:17.)

52. The Sequoia AVC Advantage 9.00H lacks any voter-verified paper ballot or independent audit trail or other way to verify that its contents are accurate. (Appel Test., 2/5 Trial Tr. at 55:19-24; Appel Report, § 2.4, at 11.) The only record of the election is the vote totals the DRE itself provides at the end of the day. (Id.) Therefore, it is a "black box" with no verifiable accuracy. (Id.) As such, like all other computers, the Sequoia AVC Advantage 9.00H DRE can be

programmed to do whatever the programmer tells it to do, and is inherently insecure and unreliable. (Appel Test., 2/5 Trial Tr. at 54:5 to 56:4; Appel Report, § 2.4, at 11.)

53. The voter interface of the Sequoia DREs at issue in this case is a panel on the front of the DRE with numerous rows of buttons programmed to correspond to different candidates or to different answers on ballot questions, covered with a mylar sheet to indicate to the voter which buttons correspond to which candidates or ballot questions. (See Appel Test., 1/27 Trial Tr. at 156:4-8, 162:23 to 163:4, 173:14 to 174:6; Appel Report, §§ 2.1-2.2, at 9-11.)

54. The voter interface provides a false sense of security, because unless the firmware in the DRE is programmed properly, there is no necessary correlation between pressing a button next to a candidate's name and the DRE actually registering a vote for that candidate. (Appel Test., 1/28 Trial Tr. at 97:2-6; Appel Report, § 2.3, at 11.)

55. There is also an alphanumeric keypad for entering text input such as the names of write-in candidates. (Appel Test., 1/27 Trial Tr. at 198:12 to 199:18; Appel Report, § 36.3, at 86.) Finally, there is an LCD text display for communication to the voter, such as the names of candidates and an indication that a vote has been cast. (See Appel Test., 1/27 Trial Tr. at 199:9-23; Appel Report, § 29.7, at 77.)

56. There is also an operator interface keyboard kept locked inside the DRE when it is not in operation. This operator panel is attached to the side of the DRE and used by election workers during elections. (Appel Test., 1/27 Trial Tr. at 157:14-20; Appel Report, § 9.2-9.33, at 29.)

D. How We Vote in New Jersey

57. The voter panel, which voters use to attempt to communicate their intended votes, consists of a 38-by-28 inch panel with 42 rows and 12 columns of buttons on it, each with a green X-shaped LED light next to it. (See Appel Test., 1/27 Trial Tr. 199:9-23; Appel Report, § 29.4, at 76.) Covering the panel is a large sheet of paper with a printed facsimile of a ballot on it, listing contests, candidates, and ballot questions, corresponding to buttons on the panel. (Id.) The paper is protected by a mylar sheet. (Id.) When the LED lights up, it shines through the paper and the mylar, so it is visible to the voter. (Id.)

58. Unless the DRE is activated, the AVC Advantage does not interpret pushes of the button as votes. (Appel Report, § 29.5, at 77.) After the DRE is activated, the voter can cast votes by pressing buttons through the paper cover, where the cover is marked for that candidate. (Appel Report, § 29.6, at 77.) When the voter does this, a green X lights up next to the candidate. (Appel Test., 1/27 Trial Tr. at 199:9-14.) Additionally, an LCD display at the bottom of the panel, which is capable of displaying letters and numbers, should display the name of the candidate and the contest when the voter presses a button to select a candidate. (See Appel Test., 1/27 Trial Tr. at 198:7-23; Appel Report, § 29.7, at 77.)

59. After the voter casts at least one vote, a large, red "Cast Vote" button, below the voter panel on the right side, lights up brightly. (Appel Report, § 29.9, at 78.) If the voter presses the "Cast Vote" button at any time after it lights up, all currently chosen votes should be tabulated, the DRE should emit a chirping sound, the LCD display under the voting panel should display the message "VOTE RECORDED THANK YOU," and the overhead light in the booth should turn off. (Appel Test.,

1/27 Trial Tr. at 201:6-14; Appel Report, § 29.10, at 78.) The DRE should then return to its inactive state. (Appel Test., 1/27 Trial Tr. at 201:16-19.)

60. In New Jersey, the normal mode of voting is to enter a polling place, and approach a table where election-board workers sit with pollbooks containing the names, addresses, and signatures of registered voters. (Appel Test., 1/29 Trial Tr. at 100:20-25; Appel Report, § 29.1, at 75.) A poll worker sits at each table, and there may also be challengers at the table, representing the two political parties, to question the eligibility of voters. (Id.)

61. The voter then countersigns the poll book, a poll worker compares the signature to the signature of record in the poll book, and gives the voter a "Voting Authority" ticket from a pad. The Voting Authority is a piece of paper approximately four inches square, which has a serial number. (Appel Test., 1/27 Trial Tr. at 158:20-25, Appel Report, § 29.1, at 75.) A stub also containing this serial number remains in the pad. (Id.) In a general election, these tickets are from the same group. But in a primary election, the ticket indicates the party in whose primary the voter is entitled to cast votes. (Appel Test., 1/27 Trial Tr. at 160:8-18; Appel Report, § 34.2, at 84.)

62. The voter then approaches another poll worker who stands next to the DRE. This poll worker takes the ticket and retains it in a manner that varies from county to county. (Appel Report, § 29.2 n.69 and accompanying text, at 75-76.) If the election is a general election, the poll worker activates the DRE simply by hitting the green "Activate" button. (Appel Test., 1/27 Trial Tr. at 160:2-7.)

63. If the election is a primary election, the poll worker activates the DRE by pressing the button associated with the voter's party and then presses the "Activate" button. (Appel Test., 1/27 Trial Tr. at 160:9 to 161:8; Appel Report, § 56.6, at 116-117; see also Section II.R for an explanation of a bug in this process that has disenfranchised New Jersey voters.)

64. In a general election, after the poll worker activates the DRE by pressing the "Activate" button, which causes the DRE to emit a barely audible chirping sound for a quarter of a second, an overhead light on the inside of the DRE's privacy curtain turns on and, if the county has chosen to enable this option, a green X appears next to each race in which the voter may vote. (See Appel Test., 1/27 Trial Tr. at 200:6-14; Appel Report, § 29.3, at 76.)

65. One of the unreliabilities of the Advantage 9.00H is that in a primary election, nothing indicates to the voter which party ballot is activated. (Appel Report, § 34.3, at 84.)

E. Fraudulent Firmware on the Sequoia AVC Advantage 9.00H DRE Can Steal Votes

1. Anyone with a Minimal Computer Engineering Background and Easily Obtained Equipment Can Create a Fraudulent Program ROM Chip

66. The computer-program firmware that controls how votes are interpreted and added in the Sequoia Advantage 9.00H resides in ROM chips on the motherboard. (Appel Test., 1/28 Trial Tr. at 20:7-10; Appel Report, § 5.2, at 21.)

67. These ROM chips are simply an off-the-shelf memory chip which Professor Appel was able to purchase on the Internet for $3.87 each. (Appel Test., 1/28 Trial Tr. at 87:3-5.)

68. Professor Appel was able to write fraudulent firmware to the program ROM chips with a commonly available device called a ROM reader/programmer, which cost $149. (Appel Test., 1/28 Trial Tr. at 87:8-13; Ex. P-16.)

69. After creating the fraudulent program ROM, Professor Appel simply replaced the legitimate ROM chip on the motherboard with the fraudulent chip and walked away. (Appel Test., 1/28 Trial Tr. at 87:14-16.) The next time the DRE was turned on, it ran the fraudulent vote-stealing program. (Appel Test., 1/28 Trial Tr. at 87:16-20.) The fraudulent vote-stealing program was now installed for perpetuity on the DRE.

70. The process for writing fraudulent firmware onto a program ROM is effectively identical to the process for writing legitimate firmware onto the same program ROM. (Appel Test., 1/29 Trial Tr. at 20:15-25.)

2. Anyone with a Few Minutes Access to an AVC Advantage can Easily Replace the Motherboard Firmware with Fraudulent Vote-Stealing Firmware

71. Professor Appel demonstrated the process for physically replacing the ROM chips on the motherboard of the Sequoia AVC Advantage 9.00H on videotape for the Court. (See generally, DVD 4 Tape 4; Appel Report, § 5.1, at 21.) Additionally, he also successfully demonstrated this same process in open court under extreme constraints as part of the State's cross examination.

72. The physical process of replacing the chip involves multiple steps, each of which is simple and can be done quickly. Professor Appel is a professor, not a burglar. (Appel Test., 1/28 Trial Tr. at 79:2-5.) However, he was able to purchase lock picking tools on the Internet for $40. (Appel Test., 1/28 Trial Tr. at 79:20 to 80:1.) Much cheaper tools are also available. (Appel Test., 1/28 Trial Tr. at 80:2-

5.) After a half-hour of instruction from a graduate student who studies physical security, he was able to learn how to pick the lock on the AVC Advantage 9.00H rapidly. (Appel Test., 1/28 Trial Tr. at 79:12-19.) On the videotape, he was able to pick the lock in less than fifteen seconds. (Appel Test., 1/28 Trial Tr. at 83:18 to 84:10; DVD 4 Tape 5, at 5:58 to 8:19.)

73. Professor Appel was then able to remove the panel covering the main circuit board by removing the ten sheet-metal screws which hold it in place. (Appel Test., 1/28 Trial Tr. at 84:11-12; Appel Report, § 5.6, at 22.) It was possible for Professor Appel to do this without disturbing the plastic strap seal on the DRE, which is supposed to both reveal and deter such tampering. (Appel Report, § 10.6, at 33-34.) Notably, one of the DREs the State provided to Plaintiffs did not even have this plastic strap seal. (Appel Report, § 10.4, at 31-32.)

3. It is Not Difficult to Replace the Firmware in the Sequoia AVC Advantage with Fraudulent Vote-Stealing Firmware

74. The firmware in the AVC Advantage is a computer program which allows election officials to install ballot definitions, enables election workers to open and close elections, translates the user's button pushes into their intended votes, and counts and remembers those votes. (Appel Report, § 3.2, at 15.) There is firmware on both the motherboard and the daughterboard. (Appel Test., 1/28 Trial Tr. at 52:20-23.) The daughterboard allows audio voting for disabled voters. (Id. at 66:1-3.)

75. The most significant vulnerability of the Sequoia Advantage 9.00H DRE is that its firmware can be replaced with fraudulent vote-stealing firmware. (Appel Test., 1/28 Trial Tr. at 47:11-14.) Professor Appel discovered many pathways

through which fraudulent firmware could be introduced into the Sequoia Advantage 9.00H DRE. (Appel Test., 1/28 Trial Tr. at 47:15-19.) Professor Appel demonstrated many of these methods in open court. (See generally Appel Test., 1/28 and 1/29 Trial Tr.)

76. One method which Professor Appel demonstrated in court involves replacing one of the four ROM chips on the motherboard with a ROM chip containing fraudulent vote-stealing software. (Appel Test., 1/28 Trial Tr. at 54:17-24.)

77. Another method he testified about was replacing the Z80 chip on the motherboard with a fraudulent version of the Z80 chip. (Appel Test., 1/28 Trial Tr. at 55:3-5; see also Testimony of Wayne Wolf, May 11, 2009 Trial Tr., 27:18 to 28:6, 31:11-33:5)[1]

4. Professor Appel Demonstrated How the Fraudulent Firmware he Created Can Alter Election Results

78. Professor Appel created vote-stealing firmware and "burned," or copied, it to a ROM chip. (See Appel Test., 1/28 Trial Tr. at 81:25 to 82:3, 87:8-11; Appel Report, § 4.1, at 16.) The purpose of this vote-stealing program was to move votes from one candidate's total to another, while not changing the total number of votes cast. (Appel Test., 1/28 Trial Tr. at 82:5-6; Appel Report ¶ 4.1, at 16.)

79. It took only two days for Professor Appel to design the fraudulent firmware he installed in the ROM chip. (Appel Test., 1/28 Trial Tr. at 85:20-25.) Professor

[1] Professor Wayne Wolf, qualified by this Court as an expert in processor design and embedded systems, among other things, testified that designing such a Z80 chip which could contain malicious vote-stealing software and evade detection, would be entirely possible for any reasonably competent computer engineer with as much as a Bachelor's degree. (Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 41:7-11.) Any contrary testimony by unqualified laypeople such as Edwin Smith or Paul Terwilliger, uncertified as experts by this Court on computer processor design or embedded systems, should be disregarded as having no probative value.

Appel modified only 122 lines of approximately 130,000 lines of Advantage 9.00H firmware. Copying the fraudulent firmware to the ROM chip takes only approximately ten seconds. (Appel Test., 1/28 Trial Tr. at 85:20-25; Ex. P-16.)

80. Professor Appel designed his vote-stealing firmware not to cheat in "Pre-LAT" or "pre-election logic and accuracy testing" mode. (See Appel Test., 1/28 Trial Tr. at 82:5-9; Appel Report, § 4.2, at 16.)

81. Pre-LAT mode is a mode in which election workers run a mock election, cast pre-selected votes, and then print out the totals to make sure the results came out as they should have. (Appel Test., 1/27 Trial Tr. at 186:19 to 187:10.) The Advantage 9.00H DRE stores in its memory an indication of whether it is in Pre-LAT or Official Election mode. (Appel Test., 1/28 Trial Tr. at 92:22 to 93:5.) Professor Appel's fraudulent firmware was able to take advantage of this feature, so the fraudulent firmware "knows" whether it is in Pre-LAT or Official Election mode. (Appel Test., 1/28 Trial Tr. at 92:22 to 93:9.) Thus, it avoids stealing votes during Pre-LAT testing. (Appel Test., 1/28 Trial Tr. at 93:6-16; Appel Report, § 4.2, at 16.) Professor Appel's fraudulent firmware only steals votes during Official Election mode. (Appel Test., 1/28 Trial Tr. at 92:19-21; Appel Report, § 4.2, at 16.)[2]

82. The fraudulent firmware designed by Professor Appel also demonstrates another method of evading detection, which would thwart attempts to detect it by testing the DRE in Official Election mode. (Appel Test., 1/28 Trial Tr. at 93:6 to 94:21;

[2] Defendants' expert witness, Dr. Shamos, agrees with Professor Appel that Pre-LAT testing is not intended to, and does not, detect fraudulent firmware. (Testimony of Michael Shamos, March 24, 2009 Trial Tr. at 72:3-6.)

Appel Report, § 4.3, at 16.) Professor Appel's fraudulent firmware waits until the twentieth vote is cast before changing the vote totals. (Id.)

83. Professor Appel could have designed fraudulent firmware to wait for 50 votes, 150 votes, or any other arbitrary number of votes before cheating. (Appel Test., 1/28 Trial Tr. at 94:4-21.) He chose twenty for the purpose of making his demonstration manageable. (Appel Test., 1/28 Trial Tr. at 94:17-21.)

84. When the voter casts the twentieth vote using Professor Appel's fraudulent firmware, the firmware goes through all the previously cast ballot images (records of votes cast) and alters half of the votes originally assigned to the H13 button so that they become assigned to the E13 button. (Appel Test., 1/28 Trial Tr. at 94:25 to 95:5.)

85. It does not matter which candidate's names are associated with these ballot positions. As long as there are candidates assigned to the buttons on the voter panel that the fraudulent firmware has been directed to manipulate, the fraudulent firmware will change the vote totals. (Appel Test., 1/28 Trial Tr. at 93:18-25.)

86. The DREs Professor Appel used to demonstrate his vote steaing program were two Sequoia AVC Advantage 9.00H DREs from Union County, configured for the Super Tuesday Presidential primary election of February 5, 2008. (See Appel Test., 1/27 Trial Tr. at 165:20 to 166:5; Appel Report, § 4.8, at 17.) He used this contest to demonstrate that the DREs are hackable when used exactly the way they are normally used in New Jersey. (Appel Report, § 4.8, at 17.) Bill Richardson was the candidate assigned to the H13 button and Dennis Kucinich

was assigned to the E13 button. (Appel Test., 1/28 Trial Tr. at 97:10-15; Appel Report, § 4.10, at 17.)

87. The demonstration of how the fraudulent firmware works was done through a series of mock elections and was shown to the Court via videotape. That demonstration is summarized below:

a. First Election:

- Professor Appel first ran a complete election using the real firmware instead of the fraudulent firmware. As part of this complete election, he first ran a Pre-LAT test. Professor Appel, as the poll worker, activated the DRE and ran a zero tape, which indicated the proper number of voters before the election (zero in all columns). For the Pre-LAT test, the "voter," Maia Ginsburg, a member of Professor Appel's research team, placed twenty votes for Democratic candidates only. Professor Appel, as the poll worker, activated the DRE between each vote for the Democratic slate. The vote total was 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. Then, Professor Appel, as the operator, finished the Pre-LAT test and printed a results tape. The tape indicated 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (DVD 3 Tape 3, at 7:50 to 20:50.)
- Also as part of the first election, Professor Appel and the "voter" cast identical votes in Official Election mode – 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. The zero tape printed at the beginning of the test showed zero votes in all columns. When Professor Appel closed the polls, the post-election printouts reflected the number of votes actually cast -- 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (DVD 3 Tape 3, at 28:10 (Zero Tape), 37:10 (Results Report).)

b. Professor Appel then Hacked the DRE:

- In the videotaped demonstration, Professor Appel then demonstrated how he was able to replace legitimate firmware with fraudulent firmware. This entire process took under seven minutes. (DVD 4 Tape 4, at 4:28 to 11:22.) First, Professor Appel picked the lock on the back of the DRE. That process took fourteen seconds. Once he gained access to the innards of the DRE, Professor Appel

unscrewed the ten screws on the circuit-board cover of the DRE. This enabled him to access the motherboard and the ROM chips on it. He then replaced the legitimate firmware ROM chip with a ROM chip containing his fraudulent version of the firmware. Finally, he closed the DRE again and screwed all ten screws back in. The DRE showed no indication of tampering. With the fraudulent firmware, the DRE was programmed to cheat in all future elections in Official Election mode. That entire process took only 6 minutes and 51 seconds.

c. The Second Election, with Vote-Cheating Malware:

- After replacing the legitimate firmware with fraudulent firmware, Professor Appel ran a second election that was identical to the first one. In Pre-LAT mode, "voters" cast 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (Appel Test., 1/28 Trial Tr. at 103:13-22; DVD 4 Tape 4, at 25:34 to 34:58.) The fraudulent firmware, which Professor Appel programmed to behave normally in Pre-LAT mode and only steal votes in Official Election mode, produced the correct totals of 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (Appel Test., 1/28 Trial Tr. at 103:13 to 104:1.) These results were also listed in the Pre-LAT report. (DVD 1, at 2:35.)
- Then, also as part of the second election, Professor Appel switched the DRE to Official Election mode. Ms. Ginsburg once again acting as "voters" cast the exact same 16 votes for Bill Richardson and 4 votes for Dennis Kucinich. (Appel Test., 1/28 Trial Tr. at 107:16 to 108:11.) After Ms. Ginsburg cast the final vote, Professor Appel turned the key in the DRE to the "polls closed" position. This caused the DRE to print out a paper results report. (Appel Test., 1/28 Trial Tr. at 108:9-11; DVD 4 Tape 4, at 40:04 to DVD 4 Tape 5, at 14:12.)
- The fraudulent firmware worked as designed. As captured on the videotape as each vote was cast, Bill Richardson's real total was 16 votes. But, the printout for the DRE showed only 8 votes for Richardson. (Appel Test., 1/28 Trial Tr. at 108:6-21.) The fraudulent firmware stole 8 of Bill Richardson's original 16 votes, leaving him with 8, and added those 8 stolen votes to Dennis Kucinich. This gave Kucinich 12 votes in total. (Appel Test., 1/28 Trial Tr. at 108:17-21.) The DRE's paper results report also showed these fraudulent totals. (Appel Test., 1/28 Trial Tr. at

108:12-15; DVD 4 Tape 5, at 13:13 to 14:12; Exs. P-20, P-21.)

88. The fraudulent firmware was meticulously crafted. Professor Appel programmed his fraudulent ROM chip to go through the DRE's ballot image files (which are the record Sequoia erroneously calls an "audit trail") and give 8 of Bill Richardson's 16 votes to Kucinich. An election official consulting the "audit trail" would get the exact result shown on the paper election result report. (DVD 4 Tape 5, at 8:29 to 14:40; see generally Testimony of Andrew Appel ("Appel Test."), February 9, 2009 Trial Tr. 20:9 to 21:8; Appel Test., 1/28 Trial Tr. at 111:25 to 112:6.) Thus, Dennis Kucinich appeared to win over Bill Richardson by 12 to 8 votes, in an election he had actually lost to Bill Richardson by 16 to 4 votes. (See Appel Test., 1/28 Trial Tr. at 108:12-21.)

89. In the Sequoia Advantage 9.00H, when each vote is cast, the legitimate firmware stores the vote in four different redundant ways:

- First, it is added to the end of the "audit trail" file in the internal memory on the motherboard. (Appel Test., 2/9 Trial Tr. at 21:19-24.)
- Second, it is added to the candidate totals on the internal memory of the motherboard. (Appel Test., 2/9 Trial Tr. at 21:24 to 22:1.)
- Third, it is added to the audit trail file on the results cartridge. (Appel Test., 2/9 Trial Tr. at 22:1-2.)
- Fourth, it is added to the candidate totals on the results cartridge. (Appel Test., 2/9 Trial Tr. at 22:2-3.)

90. Professor Appel's fraudulent firmware altered the vote totals in all four forms in which it is saved by the DRE, so that all the results appear consistent. (Appel Test., 1/28 Trial Tr. at 111:14-24.) The fraudulent firmware altered:

- the vote totals produced on the results report from the file containing the vote totals in the DRE's memory;

- the file containing the vote totals on the results cartridge;
- the ballot images in the audit file in the DRE's internal memory; and
- the ballot images in the audit file on the results cartridge.

(Appel Test., 1/28 Trial Tr. at 111:17 to 112:13.)

91. The printout and all four electronic records of the election created by the DRE are completely consistent, even though they are all fraudulent. Nothing survives the operation of the fraudulent firmware to contradict the altered results. (Appel Test., 1/28 Trial Tr. at 111:14 to 113:10.)

92. There was no evidence of tampering, and no independent means by which the totals can be audited. (Appel Test., 1/28 Trial Tr. at 121:15 to 122:5.) The fraud is not detectable. No record of the actual votes cast survives the tampering. (Id.)

93. Professor Appel demonstrated the hack of the results cartridge in the video. He took the results cartridge from the DRE and placed it into the WinEDS computer provided by Union County. The WinEDS computer did not detect the fraudulent results; it merely tabulated the fraudulent vote totals just as if they were legitimate. (Appel Test., 1/28 Trial Tr. at 121:2-6; DVD 1, 18:47.)

94. Thus, once the fraudulent firmware is introduced into the DRE and corrupts the results of the election, every record of the election will reflect the fraudulent results chosen by the creator of the fraudulent firmware. (Appel Test., 1/28 Trial Tr. at 121:15 to 122:5.) The true expression of the will of the people is gone forever and cannot ever be determined. (Appel Test., 1/28 Trial Tr. at 121:15 to 122:5.)

95. Professor Appel's fraudulent firmware demonstrates a basic tenet of computer science: A computer will do whatever it is programmed to do. The Sequoia AVC

Advantage 9.00H DRE is no exception to this rule, and can run any program any other Z80-based computer can run. (Appel Test., 1/28 Trial Tr. at 22:25 to 23:11.)

5. Fraudulent Firmware Can Cheat in a Number of Ways

96. The fraudulent firmware designed by Professor Appel waits until a certain number of votes are cast, then switches the totals of two candidates assigned to specific buttons on the front panel. (Appel Test., 1/28 Trial Tr. at 93:9-13.)

97. While this example of fraudulent firmware was based on the button positions, and ignored names, it would be straightforward to design firmware which, instead, operates based on the names of the candidates in the ballot definition. (Appel Test., 1/28 Trial Tr. at 110:16 to 111:2.)

98. Fraudulent firmware can also misrecord the voter's intent, indicating that it has counted the vote for one candidate while actually counting it for another. (Appel Test., 1/28 Trial Tr. at 110:16 to 111:2; Appel Report, § 3.3(1), at 15.)

99. Another method of cheating is to record how each voter voted in sequential order, violating voters' privacy. (Appel Report, § 3.3(3), at 15.)

100. These other methods of cheating do not present any difficult programming problems. Professor Appel could easily write programs to perform these tasks, as could anyone with the expertise of an average Bachelor's-degree-level computer scientist. (See Appel Test., 1/28 Trial Tr. at 126:13-23; Appel Report, § 7.1, at 26.) The skills for creating fraudulent firmware are similar to creating computer viruses. The existence of tens of thousands of known computer viruses is evidence of how common such skills are. (Appel Report, § 7.2, at 26.)

6. Fraudulent Firmware Can Also be Installed by Replacing the Z80 Chip on the Motherboard

101. Professor Appel, both in his Expert Report and in testimony before this Court, testified about the characteristics of Z80 chips and the ease with which it is possible to design variants of this 30-year-old chip. (Appel Test., 1/29 Trial Tr. at 21:1 to 23:12.) Plaintiffs also called Professor Wayne Wolf, an expert in processor design, to testify, who corroborated every point made by Professor Appel. (See, e.g., Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 26:21 to 29:20, 31:20 to 34:8.)

102. The Central Processing Unit ("CPU") chip that "masterminds" the AVC Advantage 9.00H is a Z80 processor, invented in 1976. (Appel Report, § 12.2, at 44.) This chip, primitive by today's standards, is easily replaced by an imitation designed to steal votes. (Appel Test., 1/29 Trial Tr. at 21:1 to 23:12.)

103. Professor Appel, in particular, has extensive experience with the very common Z80 processor spanning back to its invention in the late 1970s when, in his first employment at University of Illinois Medical School, he programmed a Z80 chip to be the controller of a Braille printer for blind people. (Appel Test., 1/29 Trial Tr. at 17:3-10.) Professor Appel has also programmed the Z80 chip to do communications functions and other computer functions. (Appel Test., 1/29 Trial Tr. at 17:1-10.)

104. The Z80 processor is very similar to many other classes of microprocessors which Professor Appel has used throughout his career. (Appel Test., 1/29 Trial Tr. at 17:11-21.) The Z80 is a CPU, which actually executes the computer programs

stored in other parts of the computer, such as, in this case, the program ROMs. (Appel Test., 1/29 Trial Tr. at 18:12 to 19:5.)

105. There is a commonly available off-the-shelf computer component called a field programmable gate array ("FPGA") that can be programmed to emulate other computer chips. (Appel Test., 1/29 Trial Tr. at 21:1-9.) An FPGA capable of emulating the Z80 retails for about $13. (Appel Test., 1/29 Trial Tr. at 21:12-19.) The Z80 processor is so old and well-known that designs to program an FPGA to emulate the Z80 are easily downloadable from the Internet. (Appel Test., 1/29 Trial Tr. at 22:4-9.)

106. Programming a $13 FPGA using this software downloaded from the Internet would result in a chip which would behave identically to a real Z80. (Appel Test., 1/29 Trial Tr. at 21:12 to 22:9.)

107. A person with a Bachelor's degree in computer engineering, and probably a third of people with Bachelor's degrees in computer science, would have the expertise to program an FPGA using the readily available Z80 emulator program. (Appel Test., 1/29 Trial Tr. at 22:10-18.) Approximately 25,000 people earn Bachelor of Science degrees in computer science in the United States every year. (Appel Test., 1/28 Trial Tr. at 78:3-5.)

108. The fake Z80 processor created by this method could easily be disguised as a real Z80 by embedding it in a one-inch-by-three-inch package resembling the plastic coating on the real Z80 processor. (Appel Test., 1/29 Trial Tr. at 23:3-7.) There are fabrication services which routinely perform such industrial prototyping, and doing so is nothing out of the ordinary. (Appel Test., 1/29 Trial Tr. at 23:8-12.)

Professor Appel contacted one of these services to get prices for packaging an FPGA in a Z80-style plastic coating, and learned that mock Z80 packaging could be obtained for $40 to $60 per unit, with a lower per-unit price for larger batches. (Appel Test., 1/29 Trial Tr. at 23:13-19.)

109. The process for creating fraudulent firmware to run on a Z80 processor would be the same as the process for creating fraudulent firmware for the program ROM chip. (Appel Test., 1/29 Trial Tr. at 20:19-25.) Once this fraudulent firmware was created, the attacker could download it onto the FPGA using an FPGA programmer device, which can be attached to a normal personal computer. (Appel Test., 1/29 Trial Tr. at 23:20 to 24:7.)

110. To replace the Z80 processor on the motherboard, the legitimate chip needs to be de-soldered and the new fake chip needs to be soldered to the motherboard. (Appel Test., 1/29 Trial Tr. at 24:8-20.) An inexpensive desoldering tool can be used to remove the solder, and a soldering iron can be used to re-solder the fraudulent Z80 processor to the board. (Appel Test., 1/29 Trial Tr. at 24:8-20, 25:11-21; Appel Report, Fig. 18, at 46.) Professor Appel has soldered computer components to motherboards on multiple occasions. (Appel Test., 1/29 Trial Tr. at 24:21-24.) Using soldering tools to replace electronic components is a basic skill in electrical engineering as well as in the repair of consumer electronics. (Appel Test., 1/29 Trial Tr. at 24:25 to 25:5.) The ability to replace electronic components is very common, even among low-level employees in the electronic industry with no formal training. (Appel Test., 1/29 Trial Tr. at 25:2-10.)

Professor Appel himself has had this ability since he was a teenager. (Appel Test., 1/29 Trial Tr. at 25:9-10.)

111. The equipment needed to desolder and re-solder electronic components to circuit boards is also readily available, and ranges from a cheap tool set available for $30 to industrial scale tools costing $650 or more. (Appel Test., 1/29 Trial Tr. at 25:11-21.)

112. The time necessary to desolder and re-solder a Z80 processor to a motherboard would be approximately ten minutes. (Appel Test., 1/29 Trial Tr. at 26:16-25.)

113. The process of creating a fraudulent Z80 chip on an FPGA would consist of two phases: first, designing the fraudulent firmware; second, actually loading it onto the FPGA. (Appel Test., 1/29 Trial Tr. at 27:1-8.)

114. Creating the fraudulent firmware would require three components, the first of which would be the software which enables the FPGA to simulate the Z80 processor. (Appel Test., 1/29 Trial Tr. at 27:9-11.) The second component would be the legitimate, unmodified firmware. (Appel Test., 1/29 Trial Tr. at 27:15-21.) The final component would be the program to be loaded into the fake Z80, designed to ignore the legitimate firmware at critical points and, instead, run the fraudulent firmware. (Appel Test., 1/29 Trial Tr. at 27:22 to 28:1.)

115. Professor Appel estimated that designing this fraudulent firmware would take between one and three months. (Appel Test., 1/29 Trial Tr. at 28:2-5.) Professor Wolf, who has more experience designing processors, corroborated this, but testified that he could do it even more quickly, and that it would take one of his

undergraduate students a total of fifty-six hours or less. (Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 34:4-8.)

116. Professor Appel is as capable of designing and installing a fake Z80 chip as he is of designing the fraudulent firmware he demonstrated to this Court.[3] (Appel Test., 1/29 Trial Tr. at 16:14-18.) He did not do it because this process alone would have taken at least the entire thirty days he had to examine the Sequoia DREs, and creating a fake Z80 completely indistinguishable from an authentic Z80 would have taken as long as six months. (Appel Test., 1/29 Trial Tr. at 28:2-5; Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 32:18 to 33:5.)

117. Professor Appel testified that it would not be possible to detect a fake Z80 processor. (Appel Test., 1/29 Trial Tr. at 28:6-9.) Professor Appel cited two studies to this effect: "Designing and Implementing Malicious Hardware," by Samuel T. King, et al., PROCEEDINGS OF THE FIRST USENIX WORKSHOP ON LARGE-SCALE EXPLOITS AND EMERGENT THREATS (LEET), April 2008; and "Trojan Detection using IC Fingerprinting," by Dakshi Agrawal, et al., IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 2007. (Appel Report, §§ 12.12-13, at 47, notes 32-33.)

---

[3] Professor Wolf confirmed Professor Appel's testimony about fraudulent Z80 chips being easy to create, and that even a college junior could create a fraudulent Z80 chip using a field programmable gate array ("FPGA".) (Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 33:9-16.) An FPGA is a readily available piece of computer equipment, and an FPGA sufficient to the task of emulating a Z80 chip and containing fraudulent firmware retails at $15.84 when purchased individually, and could be purchased more cheaply in larger quantities. (Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 34:21-24.) Professor Wolf also testified that even designing a fraudulent Z80 chip from the ground up, using Very Large Scale Integration ("VLSI") design, in which this Court certified him as an expert, would be within the expertise of computer engineers of normal skill. (Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 41:7-11.) A person with a Bachelor's or master's degree in the appropriate course of study would possess these skills. (Testimony of Wayne Wolf, May 11, 2009 Trial Tr. at 41:7-11.)

F. Once Vote Stealing Firmware is Installed in the Sequoia Advantage DREs, the Malware Can Steal Elections in Perpetuity

118. Professor Appel testified that the number of DREs that need to be hacked for an attacker to change the outcome of an election depends on the size of the election. (Appel Test., 2/5 Trial Tr. at 96:16-17.) The closer the expected election results are, the fewer the DREs that need to be hacked to alter the election results. (Appel Test., 2/5 Trial Tr. at 97:13-17.)

119. To avoid suspicion, an attacker would write a vote-stealing program that would steal no more than 20 percent of the vote from an infected DRE. (Appel Test., 2/5 Trial Tr. at 35:23-36:2)

120. Professor Appel testified that if an attacker wanted to steal an election where the expected difference between candidates was 1 percent, then the attacker would need to hack only 5 percent, or $1/20^{th}$ of the DREs, to avoid suspicion. (Appel Test., 2/5 Trial Tr. at 97:13-19.)

121. A vote-stealing program needs to change only 1 percent of the vote to alter some election results in New Jersey. (Appel Test., 2/5 Trial Tr. at 128:24-129:6.)

122. In order to alter the outcome of state-wide elections with margins closer than 1 percent, in perpetuity, an attacker would have to hack, at most, 500 DREs. (Appel Test., 2/5 Trial Tr. at 97:13-19.)

123. To alter an election that was projected to have a difference of greater than 1 percent, an attacker would need to hack more DREs. (Id.)

124. In a county-wide election where there may be only 600 or 900 DREs in use, an attacker would need to hack only 25 or 50 DREs to steal the election. (Appel Test., 2/5 Trial Tr. at 128:15-24.)

125. Local elections in the larger cities of New Jersey use only a few hundred DREs. (Id.) Professor Appel testified that to rig some of the local elections in New Jersey, an attacker would only have to hack one or two DREs. (Appel Test., 2/5 Trial Tr. at 128:24-129:6.)

126. An attacker would not need to know anything about a particular precinct to create a vote-stealing program that stole votes in perpetuity. (Appel Test., 2/9 Trial Tr. at 41:11-18.) Professor Appel testified that a simple vote-stealing program would work in every election regardless of the precinct where a particular DRE was located. (Appel Test., 2/9 Trial Tr. at 42:13-15.)

127. An attacker would have a window of several years to effectuate an attack in perpetuity. (Appel Test., 2/5 Trial Tr. at 97:23-24.)

1. It is Easy to Gain Access to the Sequoia Advantage 9.00H DREs in Use in New Jersey in Order to Install Fraudulent Firmware

128. It is easy to gain physical access to DREs in many locations in New Jersey.[4]

129. Additionally, any number of county employees has access to DREs while they are stored in county warehouses in different locations around New Jersey. (Appel Report, § 8.7, at 29; see also Sec. IV.)

130. It is not difficult to obtain DREs on which to practice stealing an election. Professor Appel testified that they are readily available to any member of the public on auction sites for very low prices. (Appel Test., 1/27 Trial Tr. at 121:12-

[4] Princeton University Professor Edward Felten was able, without much effort, to obtain physical access to such machines. They were stored in locations like unlocked churches (Testimony of Edward Felten, February 10, 2009 Trial Tr. 23:10 to 26:22), schools (id. at 33:7 to 34:3), and municipal buildings (id. at 43:2-22). For more details on Professor Felten's easy access to DREs throughout Mercer County, New Jersey, see section XX of this document.

25.) Professor Appel was able to acquire five Sequoia AVC Advantage Version 5 DREs on the GovDeals.com auction site, on which federal, state, and local government agencies auction equipment to the public, often used or surplus items. (Appel Test., 1/27 Trial Tr. at 121:6-17.) He paid only $82 for the lot. (Appel Report, § 11.7, at 42.) These DREs had originally been purchased by Buncombe County, North Carolina for $5,200 each. (Appel Report, § 11.8, at 42.) These machines are very similar to the current Sequoia AVC Advantage 9.00H machines used in New Jersey. (Appel Test., 1/27 Trial Tr. at 122:24 to 124:8.) Differences include the firmware version and the audio kit daughterboard, which does not exist on the Version 5. (Appel Test., 1/27 Trial Tr. at 122:24 to 124:8.)

2. Attempts to Keep the Source Code Secret are Useless to Prevent the Creation of Fraudulent Firmware

131. An attacker would not need Sequoia's trade-secret source code in order to design fraudulent vote-stealing firmware, because an attacker could acquire a version of the source code by reverse engineering, which is a common practice in the industry. (Appel Test., 1/28 Trial Tr. at 125:18 to 126:6; Appel Report, § 11.2, at 8, § 11.3, at 39.) Reverse engineering is a way of deducing the design of an engineered artifact from the artifact itself. (Appel Test., 1/28 Trial Tr. at 127:10-20; Appel Report, § 11.2, at 38.) For example, if General Motors bought a Ford automobile and took it apart to figure out how it was made in order to make one of its own, this would be reverse engineering. (Appel Test., 1/28 Trial Tr. at 127:10-15.) Here, reverse engineering is a way to determine the source code of the Sequoia DRE firmware by examining the contents of the program ROM chips on the DRE's motherboard. (Appel Test., 1/28 Trial Tr. at 136:5-14.)

132. Reverse engineering would be just as good as having the original source code for the purposes of creating fraudulent firmware. (Appel Test., 1/28 Trial Tr. at 128:2-10.) All one needs to reverse engineer Sequoia's source code is commonly available and inexpensive equipment, (Appel Test., 1/28 Trial Tr. at 87:3-13), a moderate level of computer knowledge, (Appel Test., 1/28 Trial Tr. at 126:18-23), and time. A person with a Bachelor's degree or equivalent experience in computer science, (Appel Test., 1/28 Trial Tr. at 130:10 to 131:5), could reverse engineer a ROM chip from the DRE's motherboard to determine its source code. (Appel Test., 1/28 Trial Tr. at 129:16 to 130:5.)

133. In 2007, Professor Appel supervised two graduate students in an examination of a Sequoia AVC Advantage Version 5 DRE, and partially reverse engineered the source code, deducing approximately 20 percent of it in two weeks. (Appel Test., 1/28 Trial Tr. at 136:6 to 137:10.) Based on the length of time it took to do this partial reverse engineering of the Version 5 DRE, and factoring the slightly larger size of the Version 9 firmware, Professor Appel extrapolated that reverse engineering the entirety of the source code for the Sequoia AVC Advantage 9.00H would be a straightforward task that could be completed in several weeks. (Appel Test., 1/28 Trial Tr. at 141:6-13.)

134. Reverse engineering source code is a routine task in computer science, and as such, it would have contributed little to Professor Appel's understanding of the Sequoia DREs to reverse engineer the entirety of the source code of the Version 9 DRE. (Appel Test., 1/28 Trial Tr. at 140:6 to 141:13; Appel Test., 2/5 Trial Tr. at 112:20 to 130:1.) By the time Professor Appel and his students had reverse

engineered 20 percent of the source code, they had learned all they needed to know. (Appel Test., 2/5 Trial Tr. at 112:2-5.) While the task is routine, it is time consuming, and would take an estimated 25 person-weeks to reverse engineer the source code for the Sequoia AVC Advantage Version 9.00H. (Appel Report, § 11.12, at 43.) Therefore, with only thirty days available for Professor Appel and his team to examine the Sequoia DREs, it would not have been an efficient or even possible use of time to devote 25 person-weeks to reverse engineering Sequoia's source code which was already available to them by this Court's order. (Appel Report, § 54.4, at 111-12.)

135. The process of reverse engineering the Sequoia firmware source code requires removing a ROM chip from the inside of the DRE. (Appel Test., 1/28 Trial Tr. at 57:6-11.) The contents of this chip are then read into a ROM reader/programmer. The ROM chip can then be replaced and the attackers can reverse engineer it at their leisure. (Appel Test., 1/28 Trial Tr. at 129:18 to 130:5; Ex. P-16.) Professor Appel and his team used a reverse-engineering software program called IdaPro for their analysis. (Appel Test., 1/28 Trial Tr. at 136:6-20; Appel Report, § 11.2, at 43.) To analyze about 35 kilobytes of the firmware with IdaPro took about two person-weeks. (Appel Test., 1/28 Trial Tr. at 137:4-9; Appel Report ¶ 11.2, at 43.) The Version 9 AVC Advantage has 320 kilobytes of firmware. (Appel Report ¶ 11.2, at 43.) Assuming the same rate of progress, the task of completely reverse engineering the Version 9 firmware would take about twenty-five person-weeks. (Id.)

136. Professor Appel's analysis of the reverse engineering process on the Sequoia DREs he purchased from GovDeals.com occurred in 2007, about a year before he got the Version 9.00H source code pursuant to the Court's order in this case. (See Appel Test., 1/27 Trial Tr. at 106:20-25; Appel Report, § 11.13, at 43.)

G. Professor Appel was Able to Defeat All Security Seals Introduced by Defendants

137. After Professor Appel completed his hack of the Sequoia Advantage for Defendants in the summer of 2008, and only weeks before the trial was scheduled to begin, the State began to introduce a variety of purported "security" measures. Defendants continued to introduce more "security" measures throughout the course of the trial.

138. Professor Appel, who has no special expertise in seals and locks, and who is not a burglar, was able to defeat all the seals presented to him by Defendants. (Appel Test., 2/5 Trial Tr. at 15:13 to 54:4.) During cross-examination, Professor Appel was able to defeat seals, break into the Sequoia Advantage 9.00H and replace the legitimate ROM chip with a fraudulent ROM chip while wearing a suit and tie, using makeshift tools, while eight lawyers and a judge scrutinized his every move.

H. The November 2008 Seals

139. In November of 2008, the State produced a number of seals proposed for use in the Advantage 9.00H DRE, including three-quarter inch cup seals, half-inch cup seals, and a Brooks padlock-style seal. (Appel Test., 2/5 Trial Tr. at 15:14-18; Exs. P-29 to P-37.) Professor Appel was able to defeat all these seals. After research and practice, he produced a certification describing how he defeated the seals, accompanied by two DVDs containing videotaped demonstrations of the

defeats. (Appel Test., 2/5 Trial Tr. at 19:11-15; Ex. P-32.) This certification and the accompanying DVDs were filed with the Court on December 1, 2008.

1. The ¾" Large Cup Seal from American Casting

140. One of the seals the State produced to Plaintiffs is a ¾" cup seal produced by American Casting. (Appel Test., 2/5 Trial Tr. at 18:15-23; Exs. 29 to 31.) A cup seal is a device intended to protect a screw from removal, in this case, one of the screws attaching the circuit board cover to the DRE enclosure. (Appel Test., 2/5 Trial Tr. at 32:19-23; Ex. P-35.) As such, the seal is readily visible to a casual observer, and Professor Appel was able to observe it in use on an Advantage 9.00H DRE while observing the closing of the polls as a member of the public. (Appel Test., 2/5 Trial Tr. at 19:2-5.) From this observation and brief Internet research, he was able to identify the seal and its manufacturer, and obtain significant information about its attributes. (Id.; Ex. P-29.) From the same website, Professor Appel could purchase these seals in any quantity for $0.75 each. (Appel Test., 2/5 Trial Tr. at 17:10-15.)

141. The installer of this seal puts the base of the seal over the screw hole, tightens the screw down, then presses the cap into the base, locking the screw in place. (Appel Test., 2/5 Trial Tr. at 16:5-8.) The cap of the seal has a serial number intended to identify it. (Appel Test., 2/5 Trial Tr. at 16:11-12.) The base has no serial number and is identical to other basic screw bases. (Id.) So, therefore, seals with different serial numbers will have identical, interchangeable bases. (Id.)

142. The purpose of this seal is to prevent removal of the screw, or at least to provide tamper evidence, but Professor Appel defeated both these purposes easily. (Appel Test., 2/4 Trial Tr. at 110:7-13; Appel Test., 2/5 Trial Tr. at 16:5-8.)

143. Professor Appel first defeated this seal by simply using a normal screwdriver to pop the cap off. (Appel Test., 2/5 Trial Tr. at 16:15-22.) Even though this destroyed the base, it did not damage the cap. (Id.) As noted earlier, the base has no serial number, so tampering cannot be detected when the destroyed base is replaced with a new base. Once Professor Appel replaced the base, he tapped the cap, which has the serial number on it, back into place. (Appel Test., 2/5 Trial Tr. at 16:11-12; Exs. P-30, P-31.) Professor Appel also found other methods of defeating this seal which damaged neither the seal nor the base. However, he did not demonstrate these attacks because he had already devised an adequate defeat of the seal. (Appel Test., 2/5 Trial Tr. at 17:10-15.)

144. Since Professor Appel's defeat of this seal, Defendants have variously claimed through counsel that New Jersey is going to cease using this seal, that it might keep using it, or that it might use it in combination with other, newer methods. (Appel Test., 2/5 Trial Tr. at 21:15-21, 16:11-22, 25:13-21.)

2. The Wire Cable Lock Seal

145. The wire cable lock seal has a metal component that looks like a padlock, and a long, braided steel cable. (P-32, ¶ 17, at 8-9.) To use it, the cable is threaded through a hole in the circuit board cover and a hole in the enclosure underneath, to tie them together. (Id.) The cable is then pushed through a hole in the "padlock," where ball bearings and a spring are supposed to lock it in place. (Id. at ¶ 17, at 9.)

146. Professor Appel defeated this seal quickly and easily by threading a #4 wood screw through a hole, enabling him to simply yank out the bottom plate of the padlock with a pair of pliers. (Id. at ¶ 18, at 9.) Professor Appel left no marks at all upon the seal in defeating it, and therefore, he could simply reassemble it when he was done, leaving no signs of tampering. (Id.; Appel Test., 2/4 Trial Tr. at 110:7-13.) This hack, on video, took 50 seconds. (Id.)

147. The State has represented through counsel that it will not be using this seal. (Appel Test., 1/27 Trial Tr. at 24:13 to 25:19.)

3. The Red Adhesive Tape with the New Jersey State Seal

148. Yet another of the State's ineffective proposed measures is red tamper-evident tape, which is supposed to make it obvious if an attacker opens the circuit board cover, because the attacker would have to peel off the tape to do so. (Appel Test., 2/5 Trial Tr. at 23:7-11.) This tape has a serial number and the seal of the State of New Jersey printed on it for identification purposes. (Appel Test., 2/5 Trial Tr. at 24:8-18.)

149. When a person peels the tape off normally, the adhesive partially comes off the tape and remains on the cover, causing the words "OPEN" and "VOID" to appear on the tape. (Appel Test., 2/5 Trial Tr. at 23:11-14.) However, Professor Appel used a heat gun, which is a device similar to a hair dryer, to warm up the tape before carefully peeling it off, and this method completely prevented the tape from indicating tampering, so that he could simply put it back on with nobody the wiser as to his tampering. (Appel Test., 2/5 Trial Tr. at 23:14-24; Appel Test., 2/4 Trial Tr. at 110:7-13.)

4. The Blue Plastic Strap Seal

150. Professor Appel defeated another seal provided by the State, a blue plastic strap seal, with an ordinary jeweler's screwdriver. (Ex. P-32, ¶ 21, at 11.) The first time Professor Appel attempted to defeat this seal, he was successful in 20 seconds. (Id.) After some practice, he demonstrated a defeat of the seal on video in about 8 seconds. (See generally DVD 4 Tape 4, at 4:28.) Professor Appel did not damage the seal in the course of removing it, so it could be easily replaced without leaving any evidence of tampering. (Id.; Appel Test., 2/4 Trial Tr. at 110:7-13.)

151. Professor Appel also easily defeated a similar seal previously used by the State, a green strap seal which was installed on one of the two Advantage 9.00H DREs which Professor Appel used to demonstrate the ROM hack. (Appel Report, § 10.4, at 33, Fig. 13; DVD 4 Tape 5, 28:33 to 32:41.)

152. During cross examination, the State presented Professor Appel with a plastic strap seal he had never practiced defeating before, and demanded that he defeat it in open court. (Appel Test., 2/5 Trial Tr. at 77:21 to 78:10.)

153. Despite this extreme disadvantage, and without proper tools, Professor Appel was still easily able to defeat this type of seal, achieving the defeat in less than nine minutes. (Appel Test., 2/5 Trial Tr. at 83:20 to 84:20.)

154. Even the State's witness, Mr. Terwilliger, believes an experienced intruder could easily replace this kind of plastic strap seal with an excellent forgery, and that the way these seals were installed on the Union County DREs is not an effective security measure. (Testimony of Paul Terwilliger, March 30, 2009 Trial Tr. at 158:20-25; Appel Test., 2/5 Trial Tr. at 89:3-9.)

155. Professor Appel would never face this situation in the real world. Professor Appel demonstrated that strap seals are readily available by producing a bag of sample plastic strap seals he received for free from American Casting. (Appel Test., 2/4 Trial Tr. at 113:19-22; Ex. P-28.) The sample bag included the same strap seal that the State had originally used on one of the Sequoia AVC Advantage 9.00H DREs from Union County which he used as demonstratives in this Court. (Appel Test., 2/4 Trial Tr. at 113:23 to 114:7; Ex. P-28.) American Casting asked Professor Appel no questions about his credentials or motivation for purchasing these seals and asking for samples. (Appel Test., 2/4 Trial Tr. at 114:15-19.)

156. After Professor Appel demonstrated how easy it was to defeat these seals, the State claimed, through counsel, that it was abandoning all of them. (Appel Test., 1/27 Trial Tr. at 24:13 to 25:19.)

I. The State's Second Wave of Seals

157. In December 2008, after Professor Appel easily defeated the seals provided by the State in November 2008, the State produced another set of seals, which Professor Appel also easily defeated. (Appel Test., 2/5 Trial Tr. at 25:10-14.) The State demonstrated the placement of these seals in a forensic evidence warehouse in Hamilton, New Jersey. (Appel Test., 2/5 Trial Tr. at 25:15-19; Ex. P-33.)

1. The ½" Small Cup Seal from American Casting

158. First, the State has speculated that it might replace the three-quarter inch cup seal Professor Appel defeated with a smaller half-inch cup seal without any serial number on it, also produced by American Casting. (Appel Test., 2/5 Trial Tr. at 26:1-11; Exs. P-34 to P-36.) Without a serial number to identify it, this seal is, to

use Professor Appel's word, "useless." (Appel Test., 2/5 Trial Tr. at 26:13-17.) Even with a serial number, Professor Appel could easily defeat this seal. (Id.)

159. Professor Appel defeated this seal before the Court using devices he made in his basement with cheap components he bought from his local hardware store, such as a $5 cold chisel he ground to a rounded shape so that it could fit under the cap of the seal. (Appel Test., 2/5 Trial Tr. at 28:11-19; Ex. P-33.) Professor Appel also modified a $10 pair of pliers so that it could grip under the cap to pull it off. (Appel Test., 2/5 Trial Tr. at 33:11-20; Ex. P-33.) This method damaged the base of the seal only and left the cap completely intact. Because the seals produced by the State do not have serial numbers on the base, the seal looked untouched. (Appel Test., 2/5 Trial Tr. at 34:8-13; Ex. P-36.)

2. The Brooks Padlock Seal

160. Another of the seals Professor Appel defeated before this Court is a blue plastic padlock, with a plastic base and a metal hasp. (Appel Test., 2/5 Trial Tr. at 37:10-13; Ex. P-34.) This device is labeled "Brooks" with a bar code and a serial number. (Id.) The State represented that this device could be used to secure the motherboard in the Advantage 9.00H DRE by placing the hasp through a hole in the corner of the motherboard which lines up with a hole in the case. (Appel Test., 2/5 Trial Tr. at 41:5-7.)

161. Professor Appel defeated this padlock device using a drill and a half-inch square steel plate screwed into an L-shaped block of wood, approximately an inch and a half long. (Appel Test., 2/5 Trial Tr. at 42:21-23.) He constructed this device in his basement using about $0.50 worth of materials. (Appel Test., 2/5 Trial Tr. at 42:25 to 43:1.) The purpose of this device is to act as a template to make it easy

to drill small holes in the lock to gain access to the spring which holds the hasp in place, while causing the least amount of damage to it. (Appel Test., 2/5 Trial Tr. at 42:9-14; Ex. P-37.) The hack itself takes only a minute or so. (Ex. P-33, ¶ 11, at 7.)

162. After drilling holes in the Brooks padlock, Professor Appel used another improvised device to release the spring which holds the hasp in place: a steel cylinder about three inches long and 5/8 inch in diameter, made into a kind of clamping device through which two pins apply pressure to the spring through the holes he drilled. (Appel Test., 2/5 Trial Tr. at 43:23 to 44:1.) Professor Appel used about $1 in materials, and spent two hours constructing this device. (Appel Test., 2/5 Trial Tr. at 44:3-5.)

163. Professor Appel spent approximately two days designing and fabricating the tools he used to defeat the small cup seal and Brooks padlock seal, without using any sophisticated machine tools. (Ex. P-33, ¶ 10, at 7.)

164. Professor Appel used the steel cylinder device he made to release the spring which holds the padlock's hasp in place. (Appel Test., 2/5 Trial Tr. at 43:18-21; Appel Certif. 1/25, ¶ 10 (picture).)

165. Before Professor Appel demonstrated his hack of the Brooks padlock seal for the Court, Professor Appel showed the Court two Brooks padlock seals. (Appel Test., 2/5 Trial Tr. at 38:14-16; Exs. P-37.) One of the padlock seals had been "hacked" and the other one was brand new. (Appel Test., 2/5 Trial Tr. at 39:1-3.) The Court examined both the "hacked" and the "new" padlock seals and declared: "For the record, they look the same." (Appel Test., 2/5 Trial Tr. at 39:4-5.)

166. After defeating the Brooks padlock seal, Professor Appel then replaced it on the block of wood he used as a demonstration tool. (Appel Test., 2/5 Trial Tr. at 45:6-7; Ex. P-37.) Indeed, the Court remarked that she could not see any difference between the padlock seal before and after the defeat demonstrated by Professor Appel. (Appel Test., 2/5 Trial Tr. at 39:4-5.)

167. On cross examination, Professor Appel also defeated this padlock seal installed on a Sequoia AVC Advantage 9.00H DRE using the same method he had previously demonstrated for the Court. (Appel Test., 2/9 Trial Tr. at 87:18-20.)

168. Another method Professor Appel devised to defeat the tamper-evident tape is to replace the authentic tamper-evident tape with counterfeit tape created with a laser printer. (Appel Test., 2/5 Trial Tr. at 24:2-5.) The attacker can simply duplicate the serial number and the seal of the State of New Jersey, which is available for download from the State's own website. (Appel Test., 2/5 Trial Tr. at 24:8-18.) The State appears to have abandoned this tamper-evident tape as a proposed security measure.

THE FOLLOWING TESTIMONY IS SUBJECT TO THE PROTECTIVE ORDER:

169. Defendants provided Professor Appel with four different kinds of security tape on December 30, 2008, with the understanding that the four different kinds of tape demonstrated various security features that interested the State. (Appel Test., 2/5 Sealed Trial Tr. at 5:4-11.)[5]

---

[5] The sealed transcripts that Plaintiffs received from February 5, 2009 are paginated the same as the trial transcripts with testimony recorded in open court on the same date. To distinguish between the two February 5, 2009 transcripts, Plaintiffs refer to the sealed testimony in the citation as "2/5 Sealed Trial Tr."

170. The four different kinds of security tape produced to Plaintiffs on December 30, 2008 were:

- White plastic tape with semi-circular and quarter-circular incisions, approximately 4 inches long by 1 inch wide, bearing the Brooks model number MRS2, (Appel Test., 2/5 Sealed Trial Tr. at 5:16-25);
- White plastic tape, approximately 5 inches long by 1¼ inches wide, bearing the Brooks model number MRS2, (Appel Test., 2/5 Sealed Trial Tr. at 7:21-23); and
- Blue tape with a bar code, bearing the Brooks model number KNR-11030, (Appel Test., 2/5 Sealed Trial Tr. at 7:1-6). The blue tape (model KNR-11030) was offered by the State merely as an example of a bar-code feature that the State is considering for future use. (Appel Test., 2/5 Sealed Trial Tr. at 7:3-9.) The State represented to the Court that it does not ever intend to use the blue tape. (Id.)
- Clear plastic tape with semicircular incisions and markings which are visible only under ultraviolet light. (Appel Test., 2/5 Sealed Trial Tr. at 8:3-8.)

171. Professor Appel was able to gain information about all these seals by examining the Brooks website, from which the Brooks product catalog can be viewed and printed by the public. (Appel Test., 2/5 Sealed Trial Tr. at 9:2-5; Ex. P-34.) Any attacker can use this publicly available information to devise defeats of the seals. (Id.)

172. Notably, he was able to gain significant information about the Brooks ultraviolet seal. Despite the State's assertions that the ultraviolet markings are "secret," Professor Appel found that the Brooks catalog contains a description of the ultraviolet feature of the clear plastic tape. (Appel Test., 2/5 Sealed Trial Tr. at 9:23-24.) The Brooks catalog also depicts a photograph of an ultraviolet flashlight used to illuminate the ultraviolet markings on the clear plastic tape. (Appel Test., 2/5 Sealed Trial Tr. at 10:1-5.) Both the tape and the ultraviolet

flashlight are commonly offered for sale to the public in the Brooks catalog and on the Brooks website. (Appel Test., 2/5 Sealed Trial Tr. at 10:3-9.)

173. This demonstrates that ultra violet markings are commonly known and advertised to the public. Any attacker could easily learn about them by going to the manufacturer's website. (Appel Test., 2/5 Sealed Trial Tr. at 10:3-9.)

174. Professor Appel purchased a similar ultraviolet flashlight, not from Brooks, but from another vendor that sells them for purposes entirely unrelated to seals. (Appel Test., 2/5 Sealed Trial Tr. at 8:11-22.) His flashlight cost $30. (Appel Test., 2/5 Sealed Trial Tr. at 8:15-16.)

175. Professor Appel defeated the Brooks 4 inch, Brooks 5 inch, and white plastic tapes in the same manner, several times before the Court. (Appel Test., 2/5 Sealed Trial Tr. at 6:2-4, 12:5:7, 12:15-18.)

176. Professor Appel did not defeat the ultra violet tape because no such tape exists; and as such it was not provided to him or to Plaintiffs or to any other expert witnesses.

177. As he demonstrated in Court, the defeat of the three types of security tape entails the removal and reinstallation of the tape without evidence of tampering. (Appel Test., 2/5 Sealed Trial Tr. at 12:19-20.) That means without perforating the semi-circular and quarter-circular incisions. (Appel Test., 2/5 Sealed Trial Tr. at 12:15-18, 13:12-14.)

178. The presence of ultraviolet markings on the clear plastic tape does not factor into Professor Appel's defeat of this seal. (Appel Test., 2/5 Sealed Trial Tr. at 12:19-21.)

179. To demonstrate the removal process to the Court for the first time, Professor Appel applied the white plastic tape seal to a piece of metal. (Appel Test., 2/5 Sealed Trial Tr. at 13:25 to 14:9; Ex. P-38.)

180. Then, Professor Appel covered the white plastic tape with a piece of ordinary, off-the-shelf, plastic packing tape from Office Max. (Appel Test., 2/5 Sealed Trial Tr. at 14:12-14.)

181. After covering the seal, Professor Appel used a heat gun to blow hot air onto the seal for approximately twenty seconds. (Appel Test., 2/5 Sealed Trial Tr. at 14:22 to 15:1.) Heat softened the adhesive of the seal so that it would peel off more readily. (Appel Test., 2/5 Sealed Trial Tr. at 15:3-5.) Either a heat gun or a hair dryer would suffice for this purpose. (Appel Test., 2/5 Sealed Trial Tr. at 14:22-25.)

182. When the tape adhesive was softened by the heat, Professor Appel used a razor blade to lift and peel back the seal from the piece of metal. (Appel Test., 2/5 Sealed Trial Tr. at 15:1-3.)

183. Although there was a minimal amount of adhesive residue left on the piece of metal after the seal was peeled back, that residue was entirely covered once the seal was reinstalled. (Appel Test., 2/5 Sealed Trial Tr. at 15:24 to 16:2.)

184. To demonstrate the reinstallation process, Professor Appel gently smoothed the peeled-back portion of the tape seal back down on to the metal plate. (Appel Test., 2/5 Sealed Trial Tr. at 19:12-18.)

185. Then, he removed the clear, plastic Office Max packaging tape that had been covering the tape seal. (Appel Test., 2/5 Sealed Trial Tr. at 13-18.)

186. The Office Max packaging tape came off easily, (Appel Test., 2/5 Sealed Trial Tr. at 19:16), because plastic tape loses some of its adhesive quality when applied to something else plastic, such as the tape seal. (Appel Test., 2/5 Sealed Trial Tr. at 6:23-25.)

187. No signs of tampering were evident after the plastic packaging tape was removed. (Appel Test., 2/5 Sealed Trial Tr. at 19:19-20.) None of the semi-circular or quarter-circular incisions on the tape were perforated. (See id.)

188. Using the techniques he demonstrated for the Court, Professor Appel also defeated all three tape seals on cross examination while they were attached to the DRE. The State used the seals to tape the circuit board cover to the side of the DRE, to tape the daughterboard box to the circuit board cover and to tape the audio ballot cartridge to the daughterboard. (Appel Test., 2/5 Sealed Trial Tr. at 13:16-21.)

189. The seals that Professor Appel was able to defeat do not materially improve the security of the Sequoia AVC Advantage DREs. (Appel Test., 2/5 Sealed Trial Tr. at 20:8-20.) The Sequoia AVC Advantage DREs remain vulnerable to attack despite the use of seals. (Id.)

190. Professor Appel's multiple defeats of the State's seals led him to conclude that from a computer security perspective, the seals failed to remediate the basic vulnerability of the Advantage 9.00H DRE to attacks. (Appel Test., 2/5 Sealed Trial Tr. at 53:24 to 54:4.) At most, the use of these devices would add minutes to the length of time it would take an attacker to compromise the DRE. (Id.)

END OF THE PROTECTED TESTIMONY

THE FOLLOWING TESTIMONY IS SUBJECT TO THE PROTECTIVE ORDER:

191. On April 9, 2009, Professor Appel observed Mr. Giles install a third set of security seals on the AVC Advantage 9.00H DRE at the Justice Complex, in Trenton, New Jersey. (Appel Test., 4/14 Sealed Trial Tr. at 4:9-15.)[6] Some of the seals that Professor Appel defeated, as well as some new seals constituted yet a third set of seals. Those seals included:

- Small cup seal with Gorilla Glue
- Large cup seal with Gorilla Glue
- Brooks Red Adhesive Tap Seal

192. The entire installation process took approximately thirty minutes. (Appel Test., 4/14 Sealed Trial Tr. at 4:16-18.)

193. In order to record the exact condition of the seals as they were being installed, Professor Appel took a series of photographs of the seals that Mr. Giles placed on the Sequoia DRE. (Appel Test., 4/14 Sealed Trial Tr. at 5:9-19; Ex. P-77.)

194. Photograph #11 of the series of photographs taken by Professor Appel depicts Mr. Giles attempting to put glue into a cup seal which was located deep in the crevice underneath the daughterboard. (Appel Test., 4/14 Sealed Trial Tr. at 6:18-22.) The photograph demonstrates the difficulty Mr. Giles encountered in attempting to place glue in the cup seal in the crevice and, consequently, the impracticality of that as a security measure. (Appel Test., 4/14 Ssealed Trial Tr. at 6:22-24.)

---

[6] The sealed transcripts that Plaintiffs received from April 14, 2009 are paginated the same as the trial transcripts with testimony recorded in open court on the same date. To distinguish between the two April 14, 2009 transcripts, Plaintiffs refer to the sealed testimony in the citation as "4/14 Sealed Trial Tr."

195. Photographs #16 and #17 in the series of photographs taken by Professor Appel depict a red tape seal affixed to the left side of the circuit board cover. (Appel Test., 4/14 Sealed Trial Tr. at 7:7-8, 8:9-10.) The photographs show some imperfections in the red seal that occurred in the process of removing the seal from the roll of tape and installing it onto the DRE. (Appel Test., 4/14 Sealed Trial Tr. at 7:8-11.) Specifically, above the letters "oo" in the word "Brooks," the adhesive came unstuck from the seal. (Appel Test., 4/14 Sealed Trial Tr. at 7:12-14.) There is also a bubble in the seal to the lower left of serial number. (Appel Test., 4/14 Sealed Trial Tr. at 8:11-12.) Finally, there are two places in the red border of the seal above the word "seal" where adhesive is missing. (Appel Test, 4/14 Sealed Trial Tr. at 8:13-14.) The appearance of the seal gives the misleading impression that someone tampered with it. (Appel Test., 4/14 Sealed Trial Tr. at 7:14-17.)

196. Photograph #22 in the series of photographs taken by Professor Appel depicts the condition of a cup seal located on the upper left corner of the circuit board cover. (Appel Test., 4/14 Sealed Trial Tr. at 9:12-21.) The photograph evidences the fact that the cup seal is not marked with a serial number, but rather only with the initials of the manufacturer, A.M.C.O. (Id.)

197. Photographs #19 and #23 in the series of photographs taken by Professor Appel depict a Brooks seal with an imperfection. Under the words "auxiliary cartridge," there appears to be a long white horizontal line, the length of the word "cartridge." (Appel Test, 4/14 Sealed Trial Tr. at 9:22 to 10:3.) Additionally, Photograph #19 depicts some adhesive from the seal which stuck onto the sheet

metal during Mr. Giles' installation of the seal. (Appel Test., 4/14 Sealed Trial Tr. at 10:8-10, 10:13-16.) The adhesive residue is visibly noticeable and gives the appearance that the seal has been tampered with when, in fact, it has not. (Appel Test., 4/14 Sealed Trial Tr. at 10:10-12.)

198. Photographs #26 and #27 depict discarded red tape seals that were damaged by Mr. Giles in the installation process. (Appel Test., 4/14 Sealed Trial Tr. at 10:23 to 11:7.) When Mr. Giles removed the first seal from the roll of tape seals, the adhesive came away damaged. (Id.) This happened a second time, and continued to happen nine consecutive times. (Appel Test., 4/14 Sealed Trial Tr. at 11:7-12.) On the tenth attempt to remove a red tape seal from the roll, Mr. Giles was more successful. (Id.) However, the tenth seal, depicted in Photograph #17, (Appel Test., 4/14 Sealed Trial Tr. at 12:22-25), is also damaged. (Appel Test., 4/14 Sealed Trial Tr. at 13:1-2.)

199. The eleventh seal that came off the red tape seal roll is depicted in Photograph #18. (Appel Test., 4/14 Sealed Trial Tr. at 13:2-6.) The eleventh seal was installed on the DRE. (Appel Test., 4/14 Sealed Trial Tr. at 13:7-11.) Photograph #18 shows that the eleventh seal is also damaged. (Appel Test., 4/14 Sealed Trial Tr. at 13:2-6.)

200. Photograph #28 depicts a log sheet where information regarding the seals, such as the serial numbers and comments could be recorded. (Appel Test., 4/14 Sealed Trial Tr. at 13:12-24.) As the photograph demonstrates, Mr. Giles did not record in the comments section that any of the seals were damaged. (Appel Test., 4/14

Sealed Trial Tr. at 13:22-24.) The log-sheet was not signed or dated. (Appel Test., 4/14 Sealed Trial Tr. at 13:25 to 14:3.)

END OF PROTECTED TESTIMONY

J. WinEDS is Unreliable and Insecure

201. WinEDS is highly insecure. (Appel Report, § 28.2, at 74.)

202. WinEDS is an acronym for Windows Election Data System. (Appel Test., 1/28 Trial Tr. at 13:9-18; Appel Report, § 27.2, at 72.) WinEDS is a software package which is used, before elections, to create ballot definition files and audio ballot cartridges, and after elections, to tabulate voting data from results cartridge. (Appel Test., 1/28 Trial Tr. at 6:9-12; Appel Report § 27.2, at 72.)

203. The WinEDS computer Professor Appel examined in this case is an ordinary Dell laptop with WinEDS software installed, formerly in use in Union County. (Appel Test., 1/27 Trial Tr. at 175:10-20; see also Ex. P-8.)

204. Insecurities in the WinEDS system include:

- "WinEDS creates administrator-level database accounts for all users";
- WinEDS "does not encrypt or authenticate database communication";
- WinEDS "does not remove database access for deactivated users";
- WinEDS "changes account usernames incorrectly";
- WinEDS "does not encrypt password change requests";
- WinEDS "retrieves the default password in the clear on every login";
- WinEDS "places the password suffix in a password entry field";
- WinEDS "displays the password suffix when resetting passwords";

- WinEDS "changes the password for the administrator incorrectly";
- WinEDS "lets any user export data from the database";
- "Data Wizard's import function does not work";
- WinEDS "does not validate a format string read from the database";
- WinEDS "accepts negative vote totals from the database";
- WinEDS "fails to check some function return codes";
- WinEDS "contains many small buffer overflows";
- WinEDS "trusts the list of precincts for which a Results Cartridge claims to report votes."

(Appel Report, § 27.4, at 73.)[7]

205. These insecurities make WinEDS "highly vulnerable to tampering, and there is no simple way to make it invulnerable." (See Appel Test., 65:7 to 66:22, 67:17 to 68:21; Appel Report § 23.15, at 68.)

1. Microsoft Windows has Well-Known Security Vulnerabilities that Can Be Exploited to Corrupt WinEDS

206. The WinEDS laptop computer examined by Professor Appel was equipped with the Microsoft Windows XP operating system and standard software such as Internet Explorer 7.0, Microsoft Office, and Windows Media Player. (Appel Test., 1/29 Trial Tr. at 62:3-4; Appel Report § 22, at 63, § 23.2, at 66.) Microsoft Windows and Internet Explorer contain security vulnerabilities continually discovered in the operating system on a month-to-month basis. (Appel Test., 1/29 Trial Tr. at 65:22-25, 66:1-3; Appel Report, § 23.3.)

---

[7] Matt Blaze, et al., "Source Code Review of the Sequoia Voting System" (July 20, 2007)http://www.sos.ca.gov/elections/voting_systems/ttbr/sequoia-source-public-jul26.pdf at 43-56.

207. Microsoft tries to "patch" these vulnerabilities, but users of the operating system should expect vulnerabilities at "any given time." (Appel Test., 1/29 Trial Tr. at 65:22 to 66:5.) These vulnerabilities expose the computer, the WinEDS election management program, and its data to an Internet attack. (Appel Test., 1/29 Trial Tr. at 69:15-24; Appel Report, § 23.1, at 65-66.)

208. Microsoft Windows employs a large variety of "services" and "protocols" to connect with the Internet. (Appel Report, § 23.6, at 67.) Each of these services and protocols are communicative devices that "constitute[] a vector" in which Internet attackers can insert malicious software onto a computer browsing the Internet. (Appel Test., 1/28 Trial Tr. at 66:14-18; Appel Test., 1/29 Trial Tr. at 69:15-24; Appel Report, § 23.6, at 67.) "One common vector that Internet scammers use to infect PCs with malware is by e-mail attacks." (Appel Report, § 23.8, at 67.) Opening a "bogus email attachment" can cause a malicious attack. (Appel Report, § 23.8, at 67.)

209. Professor Appel found that the Union County laptop did not minimize these vectors because it had a large number of services automatically enabled. (Appel Report, § 23.7, at 67.) These services include SQL Server, Universal Plug and Play, Net Logon, and Remote Registry. (Id.) Additionally, the Windows firewall was disabled, and a port scan of the WinEDS computer revealed several open Transmission Control Protocol (TCP) ports and a dozen User Datagram Protocol (UDP) ports. (Id.) All of these programs and open ports constitute potential vectors that can be opportunities to attack Windows or WinEDS. (Id.)

2. Vote-Stealing Viruses from the Internet Can Infect Computers Running WinEDS

210. When Professor Appel examined the WinEDS computer provided by the State to Plaintiffs, he was able to determine that the computer had been "regularly and continuously connected to the Internet for years." (Appel Test., 1/28 Trial Tr. at 62:11-20.) In fact, the computer had been connected to the Internet on February 5, 2008, during the Super Tuesday Presidential primary election. (Appel Test., 1/28 Trial Tr. at 62:23 to 63:4.) Professor Appel was able to determine this because when a web browser such as Internet Explorer is used to browse the Internet, it saves files in a "Temporary Internet Files" folder, which indicates the times and dates of Internet access. (Appel Test., 1/29 Trial Tr. at 61:18 to 63:24.) The WinEDS computer examined by Professor Appel had "thousands" of such files "spanning a period of years leading up to and including the primary election of February 5, 2008." (Appel Test., 1/29 Trial Tr. at 63:11-18.)

211. Both Professor Appel and all of Defendants' experts are completely in agreement that this opens the DRE to compromise by a variety of means. (See Appel Test., 1/29 Trial Tr. at 69:12 to 70:21; Testimony of Michael Shamos, March 23, 2009 Trial Tr. at 153:22 to 154:12; Testimony of Edwin Smith, March 19, 2009 Trial Tr. at 84:2 to 85:7.) Indeed, Dr. Shamos describes connecting any election-related computer to the Internet at any point in its existence as a "bad and terrible thing." (Testimony of Michael Shamos, March 23, 2009 Trial Tr. at 153:22 to 154:2.)

212. Sites visited from the Union County WinEDS computer include email, shopping, personal banking, streaming music, pictures, and checking news and sports results. (Appel Test., 1/29 Trial Tr. at 65:5-7.)

213. The WinEDS computer provided to Plaintiffs was not merely connected to the Internet, but to particular Internet services that present grave security threats. For example, the WinEDS computer had been connected to an online music service called AmpX. (Appel Test., 1/29 Trial Tr. at 66:9-18.) The client software for AmpX has vulnerabilities which allow an attacker to install malicious software on the computer, taking control of it. (Appel Test., 1/29 Trial Tr. at 67:4-9, 69:12-24.)

214. Professor Appel concluded that the Union County's WinEDS laptop computer, the WinEDS election management program, and the program's data were "severely vulnerable to attack from the Internet." (Appel Test., 1/29 Trial Tr. at 69:11-24; Appel Report, § 23.1, at 65-66.) Professor Appel discovered that the "general security configuration of the [computer] is wide open." (Appel Test., 1/29 Trial Tr. at 65:19 to 68:24; Appel Report, § 23.1, at 65-66)

215. Each visit to the different websites made the laptop computer susceptible to the ill effects of malware and malicious software. (Appel Test., 1/29 Trial Tr. at 65:22 to 66:8.) Malicious websites can exploit vulnerabilities in the operating system and have the potential to "insert viruses into the personal computer that's used to visit those websites." (Appel Test., 1/29 Trial Tr. at 65:22 to 66:8.)

216. An Internet connection and casual web browsing allows "outsiders [an opportunity to] interfere with preparation of the ballots, modify the results as they

are added up, and change the data stored in the database." (Appel Test., 1/29 Trial Tr. at 69:11-24; Appel Report, § 23.1, at 65-66.)

217. Casual web browsing is highly problematic because "untrustworthy websites can cause spyware and viruses to be downloaded onto the computer." (Appel Test., 1/29 Trial Tr. at 65:19 to 66:8; Appel Report, § 23.4, at 66.) Each visit to a website typically triggers a host of downloaded images and tracking information from advertising sites, like Double Click, Tacota, and Advertising.com. (Appel Test., 1/29 Trial Tr. at 65:9-12; Appel Report, § 23.4, at 66.) Thus, by accessing the Internet, users unknowingly leave the computer "severely vulnerable" to malicious software. (Appel Test., 1/29 Trial Tr. at 66:5-8; Appel Report, § 23.1, at 65-66.)

218. Professor Appel also found America Online AmpX Music Streaming Service installed and "regularly" used on the Union County laptop computer. (Appel Test., 1/29 Trial Tr. at 66:16-18.) This service allows someone to listen to online music. (Appel Test., 1/29 Trial Tr. at 67:1-3.) A computer security company, Symantec, has described AmpX as having a "high" security vulnerability. (Appel Test., 1/29 Trial Tr. at 66:16 to 67:9; Appel Report § 23.5, at 66.) Symantec reported that, "A successful attack would corrupt process memory, allowing arbitrary code to run in the context of the client application." (Appel Report § 23.5, at 66.)

219. AmpX can make the "entire computer" insecure and opens the possibility for an "attacker anywhere on the Internet" to "interfere and subvert the main functions of WinEDS." (Appel Test., 1/29 Trial Tr. at 69:15-24, 67:7-9.) An attacker

exploiting the AmpX security vulnerability would produce a malicious music stream. (Appel Test., 1/29 Trial Tr. at 66:16 to 67:9; Appel Report § 23.5, at 66.) The stream would then install a virus on the WinEDS computer. (Appel Test., 1/29 Trial Tr. at 66:16 to 67:9; Appel Report § 23.5, at 66.) The attacker would have access to the WinEDS computer and would be able to modify the WinEDS vote database or the WinEDS vote-counting program. (Appel Test., 1/29 Trial Tr. at 69:11-24; Appel Report § 23.5, at 66.)

220. According to logs and cache files on the Union County WinEDS computer, a user of the computer engaged in casual web browsing immediately before and after the Super Tuesday Presidential primary election of February 5, 2008. (Appel Test., 1/29 Trial Tr. at 65:12-18; Appel Report, § 23.4, at 66.) A user visited an online banking site on Election Day itself. (Appel Test., 1/29 Trial Tr. at 65:12-18; Appel Report, § 23.4, at 66.)

K. Any Election-Related Computer Connected to Both the Internet and a County's Internal Network can Corrupt the Whole Internal Network

221. Networks with Internet access allow viral propagation because "[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." (Appel Report, § 20.2 at 59.) Any one computer connected to the Internet on that network can facilitate viral propagation over the county's entire network. (Appel Test., 1/29 Trial Tr. at 70:4-10.)

222. WinEDS is a database arranged as a "client server system" and for the "proper function of WinEDS in a county, the computers generally need to be connected to each other through a network." (Appel Test., 1/29 Trial Tr. at 71:19-23, 72:1-6.)

A client server system has two parts: (1) a database server and (2) "client computers" that connect to the server. (Appel Test., 1/29 Trial Tr. at 71:25 to 72:2.) Here, a "database server contains[s] ballot and election tabulation data." (Appel Test., 1/29 Trial Tr. at 71:21-23.) The "client computers" running WinEDS interact with the results cartridges and audio ballot cartridges to communicate with the DRE and gather the election data. In order to process all the election results in a county, the client computers need to transmit data to the "server machine." This can happen through a local network. (Appel Test., 1/29 Trial Tr. at 71:19 to 72:5.)

223. A WinEDS computer connected to the network can succumb to viral infection without itself actually being connected to the Internet. (Appel Test., 1/29 Trial Tr. at 70:4-10.) "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 computers in that county's network." (Appel Test., 1/29 Trial Tr. at 70:7-10.) This can compromise "the integrity of the ballot preparation process and the integrity of the election tabulation process." (Appel Test., 1/29 Trial Tr. at 70:15-17.)

1. Results Cartridges Can be Adversely Affected by an Internet Connection

224. The results cartridge has two broad responsibilities in the election: (1) the results cartridge is used to "convey the ballot definition to the voting machine before the election" and (2) the results cartridge is used to "convey the results back to the WinEDS after the election." (Appel Test., 1/28 Trial Tr. at 6:14-19.) There is no protection against reading and writing data in the results cartridge. (Appel Report § 40.2, at 90.)

225. Before an election, a virus could "cause WinEDS to write fraudulent ballot definitions into (large-format) results cartridges." (Appel Report § 22.9, at 65.) Fraudulent ballot definitions could be designed that would miscount votes, such as by counting two votes for a candidate with a single button press from a voter. (Appel Test., 2/4 Trial Tr. at 10:13-15; Appel Report, § 43.1, at 94-95.) The AVC Advantage does not sufficiently check ballot definitions for "sanity," and therefore, will allow ballots like these, whether they are created accidentally or maliciously. (Testimony of Andrew Appel ("Appel Test."), Feb. 4, 2009 Trial Tr. at 10:13 to 11:20; Appel Report, § 43.6, at 96.)

226. After an election, a virus could "cause WinEDS to fraudulently miscount votes, when it accumulates the results from different precincts," casting the results of the election into doubt if they differed from the results on the results report printouts. (Testimony of Andrew Appel ("Appel Test."), Apr. 14, 2009 Trial Tr. at 60:15 21; Appel Report § 22.9, at 65.)

227. WinEDS would be unable, on its own, to detect the fraudulent vote totals. (See Appel Test., 1/28 Trial Tr. at 5:11-24; Appel Report, § 40.4, at 90; §§ 41.4-41.7, at 93.)

228. It is unlikely that fraudulent vote totals caused by a corrupted WinEDS would be discovered because there is no statewide policy in New Jersey for the examination of printed results reports, and results cartridges are used to determine the vote

totals at the end of each election.[8] (Testimony of Robert Giles, March 3, 2009, Trial Tr. at 161:6-9; see also Appel Test., 1/28 Trial Tr. at 5:13-24; Appel Report, § 41.4, at 93.)

L. The Daughterboard in the Version 9.00H Is Vulnerable To Attack

1. Viruses from the Internet Can Infect WinEDS Machines and then Spread to the Sequoia AVC Advantage 9.00H Daughterboard, Disenfranchising Voters

229. If a WinEDS computer is connected to the Internet, vulnerabilities in the Microsoft Windows operating system may allow attackers to take over the WinEDS computer or to install fraudulent software on the WinEDS computer. (Appel Test., 1/28 Trial Tr. at 66:14-18.)

230. Corrupting a WinEDS computer can be a vector for attacking the Sequoia DREs through the daughterboard. (Appel Test., 1/28 Trial Tr. at 65:7-13.) If a virus infects a WinEDS computer, that virus can write fraudulent firmware onto the audio ballot cartridge when it is inserted in order to create an audio ballot cartridge. (Appel Test., 1/28 Trial Tr. at 65:14-18.)

231. Flash memory is a form of nonvolatile memory, meaning that the contents of the memory do not disappear when the computer is powered off. (Appel Test., 1/28 Trial Tr. at 60:22-24.) Therefore, fraudulent firmware which replaces the legitimate firmware on the flash memory on the daughterboard will run every time the DRE is turned on. (Appel Test., 1/29 Trial Tr. at 82:16 to 84:3.)

---

[8] Notably, as discussed above, the ROM and Z80 chip hacks could not be detected even if election officials conscientiously examined and compared printed results reports with results cartridge results.

232. An audio ballot cartridge contains ballot definitions designed for use by the visually impaired. These, like normal ballot definitions, include the names of candidates and contests, but instead of printed text, the ballot data is spoken out loud so it can be heard. (Appel Test., 1/28 Trial Tr. at 7:17-19, 8:8-13, 61:12-15; Appel Report, § 19.5, at 56-57.) The audio ballot cartridge is a PCMCIA card, a credit-card sized device which fits in a type of slot standard on a laptop. (Appel Test., 1/29 Trial Tr. at 72:17-20; Appel Report, § 19.4, at 56, Fig. 19; P-10.)

2. The Daughterboard is Significantly More Vulnerable to Attack than the Motherboard

233. Replacing the firmware on the motherboard of the Sequoia Advantage 9.00H DRE requires the attacker to replace a chip on the motherboard. (Appel Test., 1/28 Trial Tr. at 63:6 to 64:10; Appel Report, § 5.1, at 21.) By comparison, an attacker can replace the firmware on the daughterboard through the audio ballot cartridge, because it is stored in rewritable flash memory. (Appel Test., 1/28 Trial Tr. at 61:10-17; Appel Report, § 19.10, at 56-57.) Thus, the daughterboard is considerably more vulnerable than the motherboard. (Appel Report, § 19.10, at 56-57.) The process to replace the firmware on the daughterboard requires no tools at all. (Appel Test., 1/28 Trial Tr. at 61:10-23; Appel Report, § 19.11, at 58.)

234. Since the audio ballot cartridge itself is a form of flash memory, it is important to distinguish between the audio ballot cartridge and the flash memory on the daughterboard. (Appel Test., 1/28 Trial Tr. at 53:3-7.) The audio ballot cartridge is a credit card sized external device programmed by a WinEDS computer and conveyed to the Sequoia DRE in order to install audio ballot definitions and

firmware. (Appel Test., 1/28 Trial Tr. at 8:8-16, Ex. P-10.) However, there is also flash memory on the inside of the Sequoia DRE, on the daughterboard. (Appel Test., 1/28 Trial Tr. at 53:3-7.)

235. When a user inserts an audio ballot cartridge into the PCMCIA slot on the DRE, under certain conditions, the contents of that audio ballot cartridge are automatically copied into the flash memory inside the DRE, even if the contents are fraudulent firmware. (Appel Test., 1/28 Trial Tr. at 61:10-17.)

236. The exact mechanism by which this occurs is discussed in "protected testimony" summarized in ¶¶ 242-259 below. The user is not warned in any way of the automatic copying mechanism, and this makes it easy to substitute a malicious virus-infected cartridge for a legitimate cartridge of another type. (Appel Test., 1/29 Sealed Trial Tr. at 6:7 to 7:6, 9:14 to 11:2, Appel Report, § 19.4, at 56, Fig. 19; P-10.)

237. Unlike installing fraudulent firmware on the motherboard, it does not require fraudulent intent to spread viruses through the audio ballot cartridge to the daughterboard. (Appel Test., 1/28 Trial Tr. at 65:18-21.) Well-meaning election workers could spread the virus inadvertently while attempting to do no more than install new audio ballot data. (Appel Test., 1/28 Trial Tr. at 65:18-21.) Confusingly, the PCMCIA cartridges used as audio ballot cartridges by Sequoia are labeled "Results Cartridge." (Appel Test., Trial Tr. at 17:11 to 18:1; Appel Report, § 19.5, at 56, Fig. 19; P-10.)

238. Professor Appel testified that as a result of a single WinEDS computer becoming infected with a virus from the Internet or from a malicious act by an "insider,"

every DRE in the county could become infected through the routine use of audio ballot cartridges, without any further intervention by the attacker. (Appel Test., 1/29 Trial Tr. at 72:25 to 73:3.)

239. Each infected WinEDS computer would subsequently infect any audio ballot cartridge inserted into the PCMCIA slot in the WinEDS computer. (Appel Test., 1/29 Trial Tr. at 73:10-21.)

240. When an audio ballot cartridge infected with the virus is inserted into an AVC Advantage DRE, the virus propagates into the internal flash memory of the audio kit daughterboard. (Appel Test., 1/28 Trial Tr. at 61:10-17, Appel Test., 1/29 Trial Tr. at 3:15-19; Appel Report, § 20.6.1, at 60.)

241. After that time, the virus resides in the internal memory of the daughterboard. If any uninfected cartridge is later installed into that DRE, the virus copies itself onto that cartridge. That cartridge is now infected. (Appel Test., 1/29 Trial Tr. at 73:14-21; Appel Report, § 20.6.2, at 60.) Also, while the virus resides on the WinEDS computer, it can copy itself onto other WinEDS computers on the same network. (Appel Test., 1/29 Trial Tr. at 73:14-21, 75:25 to 73:3; Appel Report, § 20.6.5, at 60.)

THE FOLLOWING TESTIMONY IS SUBJECT TO THE PROTECTIVE ORDER[9]:

242. Sequoia's design flaw in the AVC Advantage that enables a computer virus to jump from the audio ballot cartridge to the daughterboard is as follows (Appel Test., 1/29 Sealed Trial Tr. at 3:15-19)[10]:

---

[9] The path taken by computer viruses is not protected testimony. It is the mechanism that permits the virus to jump from the audio ballot cartridge to the daughterboard through the AUTOEXEC.BAT function that is protected.

- The Sequoia AVC Advantage daughterboard's execution environment manages the start-up of certain application programs, such as the audio voting application. (Appel Test., 1/29 Sealed Trial Tr. at 3:21 to 4:1.) The execution environment contains a file called "AUTOEXEC.BAT" that the operating system on the daughterboard normally executes as the first command. (Appel Test., 1/29 Sealed Trial Tr. at 4:2-5.) The AUTOEXEC.BAT command will start the audio voting application, but before that happens, it examines first (1) whether an audio ballot cartridge has been inserted into the cartridge slot on the daughterboard, and (2) if so, whether there is a folder on that cartridge called "ADDAUDIO." (Appel Test., 1/29 Sealed Trial Tr. at 4:12-18.)
- If there is an ADDAUDIO folder, then the AUTOEXEC.BAT program copies the contents of that folder onto the flash memory of the daughterboard. (Appel Test., 1/29 Sealed Trial Tr. at 4:19-21.) Copying what is in the ADDAUDIO folder will over-write and replace any similarly-named files on the flash memory of the daughterboard, including the very firmware of the daughterboard itself, including the audio voting application program, and including the entire execution environment. (Appel Test., 1/29 Sealed Trial Tr. at 4:22 to 5:1.)
- This type of design is commonly used in the "embedded" software systems industry. (Appel Test., 1/29 Sealed Trial Tr. at 5:5-7.) "Embedded" means a computer that is inside another device. (Appel Test., 1/29 Sealed Trial Tr. at 5:6-7.) An example of a computer embedded in another device is a microwave oven. (Appel Test., 1/29 Sealed Trial Tr. at 5:7-8.)
- The purpose of such a design is to facilitate the installation of upgrade firmware. (Appel Test., 1/29 Sealed Trial Tr. at 5:8-11.) Thus, when the voting machine is turned on, the AUTOEXEC.BAT program first searches for the presence of an audio ballot cartridge, and then searches, within that cartridge, for the presence of the ADDAUDIO folder. (Appel Test., 1/29 Sealed Trial Tr. at 5:15-23.) Once

---

[10] The sealed transcripts that Plaintiffs received from January 29, 2009 are paginated the same as the trial transcripts with testimony recorded in open court on the same date. To distinguish between the two January 29, 2009 transcripts, Plaintiffs refer to the sealed testimony in the citation as "1/29 Sealed Trial Tr."

> found, the AUTOEXEC.BAT automatically copies whatever is in the ADDAUDIO folder to the flash memory on the daughterboard itself. (Id.)

243. This design provides a convenient way for Sequoia technicians to be able to upgrade firmware to the daughterboard, such as when Sequoia changed the firmware from version 9.00G to the current version, 9.00H. (Appel Test., 1/29 Sealed Trial Tr. at 6:1-6.)

244. However, while this design might be appropriate for microwave ovens, it is not appropriate for use in situations where security is a relevant concern, such as in a Sequoia DRE. (Appel Test., 1/29 Sealed Trial Tr. at 7:13.)

245. This design mechanism is but another point of entry for the insertion of malware or viruses into the Sequoia AVC Advantage. (Appel Test., 1/29 Sealed Trial Tr. at 6:20-21.) Someone who wishes to corrupt elections can take advantage of this design to install fraudulent firmware onto the AVC Advantage daughterboard instead of a legitimate firmware upgrade. (Appel Test., 1/29 Sealed Trial Tr. at 6:15-19.) Indeed, because the mechanism operates without any additional prompts or instructions to the user, it is possible that the person installing the audio ballot cartridge would not even know that the firmware is being upgraded automatically. (Appel Test., 1/29 Sealed Trial Tr. at 6:25 to 7:6.)

246. The process of upgrading firmware through the automatic copying of the contents of the ADDAUDIO folder does not interfere with the process of audio voting. (Appel Test., 1/29 Sealed Trial Tr. at 7:7-9.) Therefore, at the same time that sound files for audio voting are being installed from the cartridge onto the daughterboard, the firmware could be upgraded, or even illegitimately replaced by the ADDAUDIO mechanism. (Appel Test., 1/29 Sealed Trial Tr. at 7:9-15.)

247. A person installing an audio ballot cartridge, who is unaware of the ADDAUDIO mechanism, could inadvertently install fraudulent firmware. (Appel Test., 1/29 Sealed Trial Tr. at 7:16-21.)

248. There are enormous implications of the ADDAUDIO design for the entire network of Sequoia DREs and WinEDS computers within a county. (Appel Test., 1/29 Sealed Trial Tr. at 7:22 to 8:21.) Fraudulent firmware in the form of a virus can jump from one component of the voting system to another. (Appel Test., 1/29 Sealed Trial Tr. at 8:2-4.) A virus can propagate from the audio ballot cartridge to the daughterboard, through the ADDAUDIO mechanism, and from the daughterboard back onto an audio ballot cartridge. (Appel Test., 1/29 Sealed Trial Tr. at 8:4-9.) A virus on the daughterboard could change the votes of disabled voters and selectively disable DREs. (Appel Test., 1/29 Sealed Trial Tr. at 10-13.) A virus that jumped from the daughterboard to an audio ballot cartridge and then to a WinEDS computer could infect other computers on the network and it could also affect the functions of the WinEDS program, such as ballot preparation and results tabulation. (Appel Test., 1/29 Sealed Trial Tr. at 8:10-16.)

249. A virus propagating in this manner could disable the entire election system or selective parts of an election system within a county. (Appel Test., 1/29 Sealed Trial Tr. at 8:17-21.)

250. There is no way to prevent a virus propagating from one component, like the daughterboard, to other components, like WinEDS computers, servers, and other DREs. (Appel Test., 1/29 Sealed Trial Tr. at 8:25 to 9:2, 9:14 to 11:6.)

251. A virus can propagate in two ways once it has been installed onto a daughterboard through the AUTOEXEC.BAT command. (Appel Test., 1/29 Sealed Trial Tr. at 9:14-16.)

252. First, a virus can write itself into a folder on an uninfected audio ballot cartridge that it would name "ADDAUDIO." (Appel Test., 1/29 Sealed Trial Tr. at 9:16-17.) If this audio ballot cartridge were later installed into a different Sequoia AVC Advantage daughterboard, then the virus would be able to jump to that daughterboard through the AUTOEXEC.BAT copying and installation command described above. (Appel Test., 1/29 Sealed Trial Tr. at 9:18-21.)

253. Once installed on an audio ballot cartridge, a virus can propagate from that cartridge into a WinEDS computer. (Appel Test., 1/29 Sealed Trial Tr. at 9:22 to 10:3.) When the virus copies files from the daughterboard flash memory to the audio ballot cartridge, it would copy files that activate a certain feature on Microsoft Windows called the "autorun" feature. (Appel Test., 1/29 Sealed Trial Tr. at 9:23 to 10:10.) The "autorun" feature permits certain devices, which plug in to ordinary computers, to start-up and run automatically without additional commands by the user. (Appel Test., 1/29 Sealed Trial Tr. at 10:4-13.) Examples of this kind of device are a CD-ROM disk or a memory stick. (Id.)

254. On the WinEDS computer from Union County that Professor Appel examined, the autorun feature, and another similar feature called "automount," were both enabled. (Appel Test., 1/29 Sealed Trial Tr. at 10:14-16.) This means that a device such as a CD-ROM or a memory stick or an audio ballot cartridge in PCMCIA format can command the computer to run a particular application

located on that device when it is plugged in to a computer. (Appel Test., 1/29 Sealed Trial Tr. at 10:17-22.)

255. When an infected audio ballot cartridge containing an "autorun" command is inserted into a WinEDS computer, the virus program on the cartridge will automatically execute and copy itself into that WinEDS computer. (Appel Test., 1/29 Sealed Trial Tr. at 10:22 to 11:6.) The virus will perform these steps without the user having to take any additional measures, such as clicking "go" or "ok." (Appel Test., 1/29 Sealed Trial Tr. at 12:10-18.) The result is a corrupted and infected WinEDS computer. (Appel Test., 1/29 Sealed Trial Tr. at 10:22 to 11:6.)

256. Creating a computer virus that jumps from an audio ballot cartridge to a daughterboard (and then to an uninfected audio ballot cartridge and from there to a WinEDS computer) is not difficult. (Appel Test., 1/29 Sealed Trial Tr. at 12:21-22.) Modifying the AUTOEXEC.BAT computer script, which is a familiar and simple computer script, could be performed by someone with experience in DOS-based computers. (Appel Test., 1/29 Sealed Trial Tr. at 12:24 to 13:1.) It would not even require someone with a Bachelor's degree level of experience or expertise to understand what to do. (Appel Test., 1/29 Sealed Trial Tr. at 13:1-3.)

257. The only way to prevent such viral propagation between daughterboard and audio ballot cartridge is to unplug the cables, including the power cable (a white and black twisted pair), that run from the daughterboard to the motherboard. (Appel Test., 1/29 Sealed Trial Tr. at 13:6-12; 14:8-23; 15:7-10.) By cutting all power, the daughterboard cannot execute the AUTOEXEC.BAT command. (Appel

Test., 1/29 Sealed Trial Tr. at 13:12-15.) If the AUTOEXEC.BAT command is not executed, the virus will not be copied. (Id.)

258. To prevent viral spread, it is not enough merely to disable the audio voting feature when designing the ballot definition in WinEDS. (Appel Test., 1/29 Sealed Trial Tr. at 13:16 to 14:1.) Even if it is specified that the audio ballot is not to be enabled in an election, the daughterboard will still turn on, because it still receives power from the connection to the motherboard. (Id.) Virus propagation on and off the daughterboard still occurs. (Id.)

259. Moreover, disconnecting the power cable from the daughterboard to the motherboard does not ensure that a virus implanted on the daughterboard will not propagate in the future. (Appel Test., 1/29 Sealed Trial Tr. at 15:7-21.) If power is reconnected to the daughterboard in a future election, the virus will come alive and propagate. (Id.)

END OF PROTECTED TESTIMONY

M. Fraudulent Firmware on the Daughterboard Affects All Voters, and the Votes of Blind Voters in Particular

260. Fraudulent firmware installed on the daughterboard can steal votes and disenfranchise voters in a number of ways. The most significant way is that it can change the votes of those voters who vote by audio, that is, blind voters or any voters who request to vote using the audio kit. (Appel Test., 1/29 Trial Tr. at 74:8-16.) The fraudulent firmware can change those votes before they are sent to the motherboard for tabulation. (Id.) The only record which election workers use to compute the vote totals is the printout generated by the motherboard computer, and the vote and ballot images from the motherboard and on the results cartridge.

Thus, disabled voters are more at risk from vote-stealing fraudulent firmware in the audio kit. (Appel Test., 1/28 Trial Tr. at § 24.4, at 69.)[11]

261. In addition to the threat to disabled voters, the vulnerability of the daughterboard to attacks can also impact the votes of non-disabled voters. (Appel Test., 1/29 Trial Tr. at 74:17-23; Appel Report, § 24.5, at 69.)

262. Viral infection of the daughterboard can disable the motherboard when the computer is first turned on, thereby selectively disabling DREs in precincts selected by the attacker. (Appel Test., 1/29 Trial Tr. at 74:17-23; Appel Report, § 24.2, at 69.)

263. The means the daughterboard uses to disable the motherboard is called a "buffer overrun" attack, which is an attack in which a user or a program returns invalid input in response to a request by a computer program, generally a longer string of data than the requesting program wants.[12] Well-written programs check input for being well-formed and refuse to accept input that would cause the program to crash, but the Sequoia motherboard firmware can be crippled by an invalid response from the daughterboard. (Appel Test., 2/4 Trial Tr. at 19:16 to 20:10.)

264. The effect of the buffer overrun in an infected AVC Advantage is that when the DRE is powered on, its motherboard will request input from the daughterboard,

---

[11] Dr. Shamos, the Defendants' expert witness, is in full agreement that this aspect of the Sequoia Advantage 9.00H DRE places the most vulnerable voters at risk of having their votes stolen. (Shamos Rebuttal ¶ 102, at 24.) Dr. Shamos' rebuttal report considers the severity of this flaw to be one of the most severe DRE flaws to date. (Id.) Finally, Dr. Shamos wrote in his rebuttal reportand testified that this severe vulnerability is so completely unacceptable that it requires "immediate remediation." (Id.)

[12] Details of this bug in redacted Appendix B of Professor Appel's Expert Report even though buffer overruns are a matter of common knowledge.

which will send a malicious message, causing it to reboot. (Id.) This cycle will repeat indefinitely, completely disabling the DRE. (Id.)

265. An attacker might disable voting machines in selected precincts because they include a preponderance of voters of the party the attacker wants to lose. (Appel Test., 2/4 Trial Tr. at 21:12-22; Appel Report, § 24.5, at 69.) As Sequoia DREs fail, long lines would form, delaying voters from casting their votes. (Id.) Further, many voters, either unable or unwilling to wait for lengthy periods of time, might leave before voting. These voters would be effectively disenfranchised.

266. In sum, there are several pathways in which viruses can propagate to and from the Sequoia AVC Advantage daughterboard. (Appel Test., 1/29 Trial Tr. at 3:2-12; Appel Report, §§ 19, 20, 21, 22, 24, and 26.)

- A virus can propagate to the daughterboard through the audio ballot cartridge or by the connector plug. (Appel Test., 1/29 Trial Tr. at 3:5-6.)
- A virus can propagate out from the daughterboard to the audio ballot cartridge. (Appel Test., 1/29 Trial Tr. at 3:7-8.)
- A virus can propagate from the audio ballot cartridge to WinEDS. (Appel Test., 1/29 Trial Tr. at 3:8-9.)
- A virus can propagate from WinEDS to the audio ballot cartridge. (Appel Test., 1/29 Trial Tr. at 3:9-10.)
- A virus can propagate from WinEDS to other WinEDS computers on the same network. (Appel Test., 1/29 Trial Tr. at 3:11-12.)

267. No genius is required for the daughterboard attack. (Appel Test., 1/29 Trial Tr. at 91:7-12; Appel Report, § 25.1, at 70-71.) It would be within the power of anyone with basic familiarity with DOS computers to write a crude virus to infect the daughterboard. (Appel Test., 1/29 Trial Tr. at 91:7-12.) An attacker with

knowledge equivalent to a Bachelor's degree in computer science could easily create a virus capable of determining what precinct it was in and disabling machines selectively. (Appel Test., 1/29 Trial Tr. at 91:12-20.)

1. Because the Advantage D10 uses the Daughterboard as its Main Computer, the D10 is Extremely Vulnerable to Fraud

268. The daughterboard on the Sequoia AVC Advantage 9.00H DRE is vulnerable to attack.[13] This makes the votes of blind voters or other voters who choose to vote on the daughterboard particularly unsafe.

269. The daughterboard is vulnerable because the firmware on the daughterboard is in flash memory on the board. (Appel Test., 4/14 Trial Tr. at 59:8-10; Appel Test., 1/28 Trial Tr. at 61:18-23; Appel Report, § 61.6, at 134.) Simply inserting a PCMCIA cartridge containing fraudulent firmware into the easily accessible slot on the outside of the DRE causes the daughterboard to automatically overwrite the legitimate daughterboard firmware with the fraudulent firmware on the cartridge. (Appel Test., 1/28 Trial Tr. at 61:10-17.)

270. A critical feature of the Advantage D10 is that, unlike the Advantage 9.00H, the main firmware in the Advantage D10 is on the daughterboard, which stores its firmware in rewritable flash memory.[14] (Appel Test., 4/14 Trial Tr. at 60:10-21; Appel Report, § 61.6, at 134.) The consequence of this is that fraudulent

---

[13] Version 9.00G of the firmware, which is used only in Hudson and Mercer Counties as of the time of Professor Appel's report, has identical vulnerabilities to 9.00H, which is used elsewhere in New Jersey. (Appel Report § 59.1, at 129.)

[14] The Sequoia AVC Advantage Version 8 also has vulnerabilities not shared by the Advantage 9.00H, as detailed by Professor Appel. (Appel Report, § 62, at 135-37.)

firmware on the D10 daughterboard can change the votes of all voters, not just blind voters. (Appel Test., 4/14 Trial Tr. at 60:10-21.)

271. Even Defendants' witness, Paul Terwilliger of Sequoia, admits that flash memory on the D10 daughterboard is unsafe because its contents are vulnerable to being changed or overwritten. (Testimony of Paul Terwilliger, March 30, 2009, Trial Tr. at 109:15-21.) Because fraudulent firmware on the daughterboard would change the votes before they were transmitted to the motherboard, there would be no way to detect the fraud.

272. Dr. Shamos, Defendants' expert witness, wrote in his Rebuttal Report that the severe vulnerability of the daughterboard is so completely unacceptable that it requires "immediate remediation," even in the 9.00H, where it only can directly steal the votes of disabled voters. Clearly, the situation is more severe in the D10, where the same bug can steal everyone's votes. (Shamos Rebuttal ¶ 102, at 24.)

273. Disturbingly, Sequoia claims not to have the source code for some of the firmware running on the daughterboard of the AVC Advantage computers. This means not even the manufacturer knows what is actually running on the DREs they sell. (Appel Report, § 54.12, at 114.)

274. As is the case with the daughterboard in the Advantage 9.00H, infecting the new Sequoia D10 DREs with fraudulent firmware requires no physical access to the DREs. An attacker would not need to perform any of the physical manipulations of the DREs or security devices demonstrated in this trial by Professor Appel and Dr. Johnston, both on videotape and in open Court. (Appel Report, § 61.6, at 134.) Infecting the D10 DREs would require no tools, and would require no

physical contact at all with even one single DRE or WinEDS computer. (Appel Report, § 61.7, at 134.) An attacker could place a single infected PCMCIA card anywhere in the stream of results cartridges, firmware upgrade cartridges, ballot definition cartridges, or any other cartridges used in the DRE, and succeed in infecting every WinEDS computer and every D10 DRE in use in the State.

275. That is, on the D10, unlike on the version 9.00H, the credit-card-sized daughterboard cartridge serves as the results cartridge; yet it is same cartridge that can carry firmware upgrades, legitimate or fraudulent. (Appel Report, § 61.4, at 133-34.)

276. This style of design is known to be defective by Sequoia which, in advertising material for the Sequoia AVC Advantage 9.00H DRE, specifically emphasized that the Version 9.00H DRE is secure because the results cartridge cannot contain firmware or other executable programs, but only data, indicating that it is insecure to do otherwise.

THE FOLLOWING TESTIMONY IS SUBJECT TO THE PROTECTIVE ORDER:

277. Professor Appel testified as a rebuttal witness and specifically rebutted the testimony given by Mr. Smith about certain Sequoia-recommended "hardening procedures" for its computer systems to protect against the spread of computer viruses. (See generally Smith Test., 3/18 Trial Tr. at 48, 112:8 to 127:19.) One such hardening technique that Sequoia recommends is reformatting the hard disk, another method is creating isolated networks. (Smith Test., 3/18 Trial Tr. at 121:16, 118:6-8.)

278. Sequoia's manual, "Sequoia Voting Systems Election Management System Reformatting and Reinstallation Guidelines," describes, among other things, the

two different types of protection against viral infiltration which Mr. Smith identified: (1) reformatting and reinstallation and (2) isolated networks. (Appel Test., 4/14 Sealed Trial Tr. at 18:10-12, 20:23 to 21:2; 23:6-11; Ex. P-78.)

2. Reformatting and Reinstallation

279. Reformatting a hard disk, wiping the disk drive of the computer system entirely clean, is a practice in the field of computer security to remove any potential computer viruses hiding in the operating system. (Appel Test., 4/14 Sealed Trial Tr. at 18:10 to 19:3.) Once the hard disk has been reformatted, clean copies of all the software and configuration information are reinstalled on the hard drive. (Appel Test., 4/14 Sealed Trial Tr. at 19:1-6.)

280. Mr. Smith testified that the procedure is automated and would take a medium-sized county of several hundred thousand voters approximately four hours to complete. (Smith Test., 3/18 Trial Tr. at 126.)

281. The bulk of the Sequoia manual, approximately eighty-eight pages, is dedicated to the explication of the reformatting and reinstallation hardening procedures. (Appel Test., 4/14 Sealed Trial Tr. at 23:5 to 24:1.)

282. The many steps required to correctly reformat and to securely reinstall all of the necessary software and configuration information are not easy to implement and require a significant amount of expertise in information systems administration. (Appel Test., 4/14 Sealed Trial Tr. at 24:3-7.) First, a master disk must be created by following the steps in Chapters 2 through 4 of the Sequoia manual. (Appel Test., 4/14 Sealed Trial Tr. at 24:14-19.) This master disk is then applied to every single WinEDS client and server machine using the steps described in the Sequoia manual in Chapters 5, 6, 7, and 9. (Id.)

283. There are a total of 332 individual steps which must be taken to create a master disk. (Appel Test., 4/14 Sealed Trial Tr. at 27:1-19.) Professor Appel estimated the amount of time it would take to follow and implement the 332 steps to be 26.7 hours. His calculations appear on a spreadsheet entered into evidence as Ex. P-79. (Appel Test., 4/14 Sealed Trial Tr. at 27:19-21; Ex. P-79.)

284. The same master disk cannot be used from county to county because all counties do not uniformly have the same computer equipment running the WinEDS network. (Appel Test., 4/14 Sealed Trial Tr. at 27:22 to 28:19.) Creating the master disk depends in part on the particular county's network configuration, equipment, and the specific details of the local installation. (Id.) Thus, one master disk will vary from another depending the county's equipment and installation details. (Id.)

285. Moreover, a master disk may not be useable on all of the servers and client computers within a given county. (Appel Test., 4/14 Sealed Trial Tr. at 28:20 to 29:2.) If the client and server computers vary in their internal hardware configurations, which would happen if they were purchased at different times or from different vendors, then a single master disk may not work. (Appel Test., 4/14 Sealed Trial Tr. at 28:20 to 29:9.) In that case, multiple master disks would have to be created from scratch, each from the 332-step process, each taking approximately 27 hours. (Appel Test., 4/14 Sealed Trial Tr. at 29:7-13; 29:16 to 30:4; see also Ex. P-79, at 3-4, 3-8, A-1, A-21, A-23.)

286. Thus, depending on the details of the hardware configuration of the actual computer running WinEDS and hardware configuration of the network and the

network routers that connect the WinEDS system together, the steps needed to be done to create the master disk will vary, and if different counties have somewhat different configurations of their WinEDS systems or if the WinEDS hardware was acquired at different times, then separate master disks will be required. (Appel Test., 4/14 Sealed Trial Tr. at 33:2-11.)

287. The creation of the master disk as the first step in the reformatting and reinstallation procedures requires a significant amount of expertise in information systems administration or computer network security. (Appel Test., 4/14 Sealed Trial Tr. at 33:12-21.) Sequoia "strongly recommend[s] that a member of the IS team or someone experienced in building servers be consulted prior to attempting a server rebuild." (Appel Test., 4/14 Sealed Trial Tr. at 34:1-4 (quoting section 3.2.1 of the Sequoia manual.)) The instructions contained in the Sequoia manual assume a sophisticated understanding of what certain terminology means and what the import of certain configuration decisions would be in order to successfully follow the instructions to create a secure system that works. (Appel Test., 4/14 Sealed Trial Tr. at 34:5-11.)

288. Even after completing the 332 steps necessary to create a master disk, the reformatting and reinstallation procedure involves an additional 127 distinct steps to harden the WinEDS system from viral infection. (Appel Test., 4/14 Sealed Trial Tr. at 34:22 to 35:1; 42:9-11.)

289. After the master disk is created, the next step in the process is to apply the master disk to each of the WinEDS client computers and WinEDS server computers installed in a county's election infrastructure. (Appel Test., 4/14 Sealed Trial Tr.

at 35:1-4.) That process entails following the instructions in Chapters 5, 6, 7, and 9 of the Sequoia manual first to apply the master disk and then to install clean copies of the software back onto the reformatted client computers, and finally to adjust the security configurations of the computers to be more secure than the defaults provided by Microsoft. (Appel Test., 4/14 Sealed Trial Tr. at 35:6-14, 37:22 to 38:2.)

290. Chapter 5 of the Sequoia manual describes the procedures for installing the master disk and the various other software disks such as SQL server and Adobe Acrobat. (Appel Test., 4/14 Sealed Trial Tr. at 38:25 to 39:2.)

291. Chapter 6 of the Sequoia manual explains how to install the WinEDS software on the server computer. (Appel Test., 4/14 Sealed Trial Tr. at 39:14-16.)

292. Chapter 7 of the Sequoia manual explains how to install the WinEDS software on the client computers. (Appel Test., 4/14 Sealed Trial Tr. at 39:16-17.)

293. Chapter 9 of the Sequoia manual describes how to adjust the security settings of the Microsoft Windows operating system so that many insecure features are turned off. (Appel Test., 4/14 Sealed Trial Tr. at 39:20-23.) Specifically, section 9.1 identifies approximately ninety different adjustments that have to be made to the Microsoft Windows security settings. (Appel Test., 4/14 Sealed Trial Tr. at 40:14-23.)

294. Although Sequoia provides a software program that makes those ninety adjustments automatically, (Appel Test., 4/14 Sealed Trial Tr. at 40:20-22), to apply the automated software that Sequoia provides requires an additional thirty procedural steps. (Appel Test., 4/14 Sealed Trial Tr. at 40:18 to 41:11.)

295. In total, to apply the Sequoia hardening guidelines would require performing a total of 459 distinct steps that cannot be automated using the Sequoia software program, and it would take several business days to complete the process from start to finish. (Appel Test., 4/14 Sealed Trial Tr. at 42:15-20.) The 459 total steps described in the Sequoia manual in Chapters 2 through 4, and 5, 6, 7, and 9 are ones which actual humans need to perform on the computers to harden the WinEDS system. (Appel Test., 4/14 Sealed Trial Tr. at 46:20 to 47:2.)

296. If the client work stations are thereafter connected to the Internet, there is a danger that the computers could be infected by viruses. (Appel Test., 4/14 Sealed Trial Tr. at 44:13-14.)

297. Professor Appel testified that in his expert opinion, the reformatting and reinstallation procedures should be performed at least once per year before each major election cycle. (Appel Test., 4/14 Sealed Trial Tr. at 44:20 to 45:10.) In contrast to Mr. Smith's testimony that the hardening procedures would take only four hours, (Smith Test., 3/18 Trial Tr. at 126:16-25), Professor Appel testified that implementing the Sequoia hardening guidelines is a lengthy, laborious, and time-consuming process, that requires a knowledge of computer systems administration. (Appel Test., 4/14 Sealed Trial Tr. at 47:2.)

3. Isolated Networks

298. Professor Appel also testified in rebuttal to Mr. Smith's assertions about isolated networks. According to Mr. Smith, counties should protect against viral spread by implementing redundant, isolated networks.

299. In section 8, the Sequoia manual discusses sources of viral contamination for the WinEDS system. (Appel Test., 4/14 Sealed Trial Tr. at 19:7-10; Ex. P-78, at 8-1.)

The manual reads, in pertinent part, that "[t]he major virus and spyware threat to an isolated WinEDS 3.1 environment comes from mobile storage devices and media, including but not limited to results cartridges, USB storage devices, CF/SD/XD storage devices, mobile hard disks and CD/DVD disks." (Appel Test., 4/14 Sealed Trial Tr. at 19:24 to 20:3; Ex. P-78, at 8-1.) In the foregoing passage, "mobile storage devices and media" refers to such things as USB memory devices and cartridges that contain memory and which can be plugged in to computers. (Appel Test., 4/14 Sealed Trial Tr. at 20:4-8.) These portable devices can carry viruses that can install themselves into computers such as those running WinEDS. (Appel Test., 4/14 Sealed Trial Tr. at 20:10-14.)

300. The term "isolated," as used in section 8 of the Sequoia manual, refers to a state of being unconnected to a network, such as the Internet. (Appel Test., 4/14 Sealed Trial Tr. at 20:15-18.) When a computer is connected to the Internet, it is subject to many virus and spyware threats, but even when the computer is unconnected, or "isolated," there remain threats from viruses and spyware described in section 8 of the Sequoia manual. (Appel Test., 4/14 Sealed Trial Tr. at 20:18-22.)

301. To be most effective isolated networks requires the use of three separate servers and possibly up to three networks to administer the election functions. (Appel Test., 4/14 Sealed Trial Tr. at 21:6-9.) An isolated network consists of a database "server" computer and various "client" work stations connected to it by a network router. (Appel Test., 4/14 Sealed Trial Tr. at 22:12-14.) The ballot preparation or tallying functions are performed on the client work stations which are in regular

communication with the server computer. (Appel Test., 4/14 Sealed Trial Tr. at 36:8-24.) The server maintains the actual ballot and election results information and the client computers access the server for that information. (Id.)

302. As described in the Sequoia manual, one isolated server and client work stations would be for the purpose of preparing ballots before an election. (Appel Test., 4/14 Sealed Trial Tr. at 21:9-11.) A second isolated server and client work stations would be for the purpose of tallying election results. (Appel Test., 4/14 Sealed Trial Tr. at 21:11-12.) A third isolated server would be kept as a back-up network that can be used for one of the other two purposes. (Appel Test., 4/14 Sealed Trial Tr. at 21:24 to 22:2.)

303. Sequoia recommends that these three servers be isolated from each other and from the Internet so that viruses cannot easily propagate from one function (preparing the ballot) to the other function (tallying the results). (Appel Test., 4/14 Sealed Trial Tr. at 21:12-15.)

304. To implement Sequoia's primary recommendation would require counties to triple their cost by purchasing three entire networks. (Appel Test., 4/14 Sealed Trial Tr. at 22:14-17.) At present in New Jersey, each county has only one network and one server. (Appel Test., 4/14 Sealed Trial Tr. at 22:22 to 23:1.)

305. If three isolated networks are too costly, Sequoia recommends two separate networks. (Appel Test., 4/14 Sealed Trial Tr. at 22:15-21.) Dropping the back-up network, Sequoia maintains that counties should isolate and keep separate the ballot preparation and results tallying functions. (Id.) This method reduces the

cost somewhat from triple to double what counties would have to pay to institute the Sequoia recommendations. (Appel Test., 4/14 Sealed Trial Tr. at 22:20-25.)

N. Hardening Techniques Are Irrelevant in a Software Independent System

306. All of the costs and the time-consuming efforts to implement the Sequoia hardening guidelines are unnecessary in software independent voting systems. (Appel Test., 4/14 Sealed Trial Tr. at 47:3-9.) Software independence is trust in election results without having to trust that a particular piece of software operated in a particular way. (Appel Test., 4/14 Sealed Trial Tr. at 47:8-12.) Here, software independence equates to a voter verified paper ballot. (Appel Test., 4/14 Sealed Trial Tr. at 47:13-15.)

307. Software independence applies to both the firmware inside each DRE and to the election management software, such as WinEDS. (Appel Test., 4/14 Sealed Trial Tr. at 47:13-20.) As to the firmware, a voter verified paper ballot serves as a check on the software of the DRE. (Appel Test., 4/14 Sealed Trial Tr. at 47:16-17.) Election officials can concretely determine whether the DRE added up the votes correctly when compared to a voter-verified paper ballot. (Appel Test., 4/14 Sealed Trial Tr. at 47:15-18.)

308. While it is sound practice to run a clean and secure network installation like that described in the Sequoia manual, it is also possible to trust the results of an election without having to undergo the time-consuming and cumbersome hardening procedures Sequoia recommends. (Appel Test., 4/14 Sealed Trial Tr. at 48:6-11.)

309. A system that allows for software independence, as required by Title 19 (and as will be discussed further below), provides the New Jersey electorate with

confidence that the State's 11,000 Sequoia DREs operate without viral infection. (See Id.)

END OF PROTECTED TESTIMONY

O. Design Errors and Programming Bugs Make the AVC Advantage Unreliable and Insecure

1. Vote Data is not Electronically Authenticated, Making it Vulnerable to Tampering

310. Sequoia's promotional literature makes misleading claims that the AVC Advantage DREs use "cryptographic" means of ensuring security of vote data. (Appel Test., 2/4 Trial Tr. at 56:18 to 57:19; Appel Report, § 39.2, at 88; Sequoia Voting Systems, Inc., AVC Advantage Security Overview (2004).) However, in actuality, the means Sequoia uses to verify vote data are woefully inadequate for their stated purpose, and not "cryptographic" at all. (Appel Test., 2/4 Trial Tr. at 56:18 to 57:19; Appel Report, § 39.2, at 88; § 39.6, at 89.)

311. There are mathematical methods to ensure data integrity, which are known as "digital signatures." The National Institute of Standards and Technology promulgates specifications for valid digital signatures. (Appel Report, § 39.3, at 88-89.) However, the Sequoia AVC Advantage 9.00H DRE doe no such thing. (Appel Test., 2/4 Trial Tr. at 57:5-19; Appel Report, § 39.6, at 89.)

312. Indeed, the methods used by Sequoia to verify the accuracy of the vote data is so utterly insufficient that not only will it fail to detect deliberately modified data, but it will even fail to detect some inadvertent corruption. (Appel Test., 2/4 Trial Tr. at 60:15 to 62:18; Appel Report, § 39.8, 89.)

313. In fact, the methods used by Sequoia to detect inadvertent corruption of data has been obsolete for over forty years, and therefore, does not even reliably do its

intended task. (Appel Report, § 39.8, at 89 n.82.) The unsuitability of the method used by Sequoia for testing data integrity has been known since at least 1961, and better methods have superseded it. (Id.)

314. For example, the methods used by Sequoia are completely incapable of detecting Professor Appel's rather simple fraudulent firmware. He was able to defeat the detection mechanism with no difficulty whatsoever. Any other competent programmer could similarly evade detection.

P. Sequoia's Sloppy Software Practices Leave Voters Vulnerable to Fraud and Disenfranchisement

1. Sequoia's Sloppy Software Practices Can Lead to Error and Insecurity

315. Professor Appel has examined the source code for Sequoia's firmware for the AVC Advantage 9.00H. (Appel Test., 1/29 Trial Tr. at 116:24 to 117:1.) The AVC Advantage version 9.00H software consists of almost 130,000 lines of source code (including comments and empty lines) in over 700 source files. (Appel Test., 1/29 Trial Tr. at 117:14-16; Appel Report, § 51.2, at 106.)

316. Professor Appel determined that the following substantial changes made to the AVC Advantage firmware affect the accuracy, efficiency, or reliability of the machine:

Version	Date	Notable 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 and minor changes
8.00A	1998	mostly documentation changes
8.00B	1998	bug fix

9.00	2003	FEC modification requests; audio voting
9.00C	2003	bug fixes; update to FEC coding standards
9.00D, E	2003	
9.00F, G	2004	
9.00H	2005	a few changes related to audio voting and/or FEC requirements
10	?	Daughterboard computer now "main CPU"
10.5	?	Voter-verified paper ballot?

Professor Appel concluded that the many changes in the different AVC Advantage models allow the machine to use different methods to handle ballots and count votes. (Appel Report, ¶ 60.5).

317. The AVC Advantage firmware is programmed in two different computer languages. (Appel Test., 1/29 Trial Tr. at 117:13-14.) Most of it is in C, and about 25,000 lines of it are in Z80 assembly language. (Appel Test., 1/29 Trial Tr. at 118:1-5.)

318. C is a language for writing source code that is readable, writable, and comprehensible by human beings familiar with the language. It can also be compiled into machine code. (Appel Test., 1/29 Trial Tr. at 118:9-14.)

319. Z80 assembly language is similar to machine language, and the process of converting it into machine language is more direct. (Appel Test., 1/29 Trial Tr. at 118:15-22.) It is used for low-level operations that can't easily be expressed in higher level languages like C. (Appel Test., 1/29 Trial Tr. at 118:19-22.)

320. The C programming language version used to program the Advantage 9.00H DRE is an obsolete 1970s version. (Appel Test., 1/29 Trial Tr. at 18:7-15; Appel Report, § 51.7, at 107 n. 96.) As a result, modern compiler tools that

automatically detect some programming errors are unusable with this code. (Appel Report, § 51.7, at 107.)

321. Comments in the Sequoia Advantage source code with programmers' initials indicate that at least a dozen different people have made myriad changes to the source code over a period of nearly twenty years, from 1987 to 2005. (Appel Test. 1/29 Trial Tr. at 135:12-14; Appel Report, § 51.2, at 106.)

322. Professor Appel, in his examination of the Sequoia Advantage source code, noted numerous flawed procedures that negatively impact the security and reliability of the Sequoia DREs by making the software more susceptible to bugs. (Appel Test., 1/29 Trial Tr. at 127:5-9.) A bug is a programming error, usually inadvertent, that causes the program to malfunction in some way or to become more vulnerable to attacks. (Appel Test., 2/4 Trial Tr. at 5:25 to 6:2.)

323. Bugs and sloppy software practices in DREs present a more serious concern than bugs in other applications, like word processors, since bugs in DREs can compromise the integrity of elections. (Appel Test., 1/29 Trial Tr. at 127:25 to 128:7.)

324. In Professor Appel's examination of the Sequoia source code, he was able to determine numerous substandard practices engaged in by Sequoia which impacts the security and reliability of the AVC Advantage 9.00H DRE. (Appel Test., 1/29 Trial Tr. at 119:20 to 120:15.) Standard, preferred software engineering practices serve a number of purposes, among them ensuring that source code can be understood by the people who actually have to use and revise it. (Appel Test., 1/29 Trial Tr. at 119:4-14.)

325. When source code is written clearly, well, and in conformance with best practices, the resulting programs are more reliable and understandable, and less vulnerable to tampering. (Appel Test., 1/29 Trial Tr. at 119:15-19.) Practices used by Sequoia in creating their source code increase the chances that programmers will make mistakes and the chances that these mistakes will slip through review and certification processes. (Appel Test., 1/29 Trial Tr. at 119:24 to 120:10; 139:17 to 140:3; Appel Report, § 51.1, at 106.) This means the DREs are not only more likely to miscount votes, but are also more vulnerable to attack. (Appel Test., 1/29 Trial Tr. at 119:20 to 120:5.) These deficient practices are inconsistent with the creation of computer applications in which reliability and security are of great importance. (Appel Test., 1/29 Trial Tr. at 120:6-10.)

326. The source code suffers deficiencies including, but not limited to multiple versions of computations, inconsistent naming conventions, frequent use of literal numeric values ("magic numbers"), subtle linkages among status values, numerous global variables, generic and undescriptive names, names that differ in only a single character, inconsistent declarations for external data objects, and subtle dependencies on datatypes and other properties. (Appel Test., 1/29 Trial Tr. at 124:20 to 132:6; Appel Report, § 51.4, at 106-07.)

327. Further, the source code reflects an incomplete attempt in 2001 to bring the source code into compliance with the FEC guidelines. (Appel Test., 1/29 Trial Tr. at 132:7-18.) This involved altering a third of the source code files. (Appel Test., 1/29 Trial Tr. at 133:3-6; Appel Report, § 51.5, at 107.) The evidence that the purpose of these changes was to bring the source code into compliance with FEC

standards is reflected in comments in the source files, where programmers often leave explanations of the changes they have made. (Appel Test., 1/29 Trial Tr. at 133:10-15.)

328. Evidence that this attempt to bring the source code up to FEC standards was incomplete is the use of the "Do-While (False)" construct. (Appel Test., 1/29 Trial Tr. at 136:25 to 138:6.) This software practice is prohibited by the 2002 Federal Election Commission Guidelines. (Federal Election Commission, Voting System Standards of 2002, § 4.2.4(b.)) There are about fifty occurrences of the use of this construct in the Sequoia Advantage source code. (Appel Test., 1/29 Trial Tr. at 138:5-6; Appel Report, § 51.6, at 107.)

329. Another example of a poor and sloppy software practice that actually impacts the accuracy and reliability of the Sequoia AVC Advantage 9.00H DRE is the use of multiple versions of computations. (Appel Test., 1/29 Trial Tr. at 124:18-21.) The proper practice for using the same calculation in different places is that the code author writes the code to do the computation once. Every time this computation is needed, the exact same code is used to execute it. If it is done properly, a change needs to be made in only one place. (Appel Test., 1/29 Trial Tr. at 124:22 to 125:3.) By comparison, Sequoia frequently creates different code in multiple places, all to perform the same calculation. (Appel Test., 1/29 Trial Tr. at 124:23 to 125:14.) This practice makes it very difficult to ensure that things are done consistently. (Appel Test., 1/29 Trial Tr. at 125:6-8.) It also makes updating the software more difficult, since updating it requires hunting down the

many locations where the same computation is made, and fixing each computation separately. (Appel Test., 1/29 Trial Tr. at 125:9-14.)

330. Another problem with the source code is the use of inconsistent naming conventions. (Appel Test., 1/29 Trial Tr. at 125:15-24.) In source code as voluminous as that in the Sequoia AVC Advantage 9.00H DRE, inconsistently naming similar things can lead to confusion. (Id.) Where there are problems, they are considerably more difficult to fix, because subsequent engineers face difficulties in comprehending the source code and its functionality. (Id.)

331. The Sequoia software frequently uses literal numeric values rather than variables. (Appel Test., 1/29 Trial Tr. at 125:25 to 126:5.) Again, this practice makes it very difficult to figure out what the source code actually means. (Appel Test., 1/29 Trial Tr. at 126:14-18.) Not only is source code written in this way more likely to contain bugs, but those bugs will be much more likely to go undetected, [and be much more difficult to fix when they do arise.] (Appel Test., 1/29 Trial Tr. at 121:20 to 122:3; Appel Report, § 51.8, at 107-08.)

332. At least one of these bugs, the option-switch bug, which is discussed in a separate section, has in fact already changed the vote totals in primary elections in New Jersey. (Appel Test., 1/29 Trial Tr. at 160:5-9; see also infra section II.R.)

333. Another example of a sloppy practice that Sequoia engages in is subtle linkages among status values. Often, parts of a program, upon completion or error, report back to the other part of the program, which invoked them, with a status value, intended to explain what happened. Ambiguity in these results can lead to

confusion. (Appel Test., 1/29 Trial Tr. at 130:14-24.) A bug of this sort has led to errors in vote totals in New Jersey. (Appel Test., 1/29 Trial Tr. at 130:14-24.)

334. Another sloppy practice which occurs frequently in Sequoia's source code is the use of excessive numbers of global variables. (Appel Test., 1/29 Trial Tr. at 130:25 to 131:12.) These are variables which can be accessed and altered by multiple parts of the program. (Id.) The preferred practice is to use local variables, which can only be accessed by the subroutine which needs to use them. (Id.)

335. Sequoia also often uses generic, nondescriptive variable names. This practice is considered harmful because, again, it makes it more difficult to ferret out bugs or to change the program later. (Appel Test., 1/29 Trial Tr. at 131:13-21.)

336. Another flawed naming convention involves using variables the names of which differ by only a single character, again increasing confusion. (Appel Test., 1/29 Trial Tr. at 131:22 to 132:2.)

Q. Sequoia's Use of Unexamined Third Party Software Means Even Sequoia Has No Idea What is Actually Running on its DREs

337. During Professor Appel's lengthy attempts to get Sequoia to comply with this Court's order to produce its source code, Sequoia claimed, and claims to this day, that the company does not have the source code to critical components of the firmware running on the 9.00H DREs. (Appel Test., 1/29 Trial Tr. at 149:11 to 150:5; Appel Report, § 54.12, at 114.)

338. The components to which Sequoia does not have source code are either created by third parties contracted by Sequoia to provide components, or are off-the-shelf products. Known third-party sources for software inside the Advantage 9.00H

include Sunrise, Datalight, Microsoft, IBM, General Software, and one vendor whose identity is a mystery, unknown even to Sequoia. (Appel Test., 1/29 Trial Tr. at 147:4 to 148:3; Appel Report, § 54.12, at 114.)

339. These practices are completely inconsistent with security or reliability. Effectively, what this means is that the Sequoia AVC Advantage series is running software unknown even to its manufacturer. (Appel Test., 1/29 Trial Tr. at 148:19-25; Appel Report, § 54.13, at 114.) As such, for all anyone knows, it could even be running fraudulent programs that can steal elections. (Appel Test., 1/29 Trial Tr. at 148:19-25; Appel Report, § 54.13, at 114.)

R. Sloppy Programming and Computer-Programming Errors Have Actually Disenfranchised New Jersey Voters

1. Party-Affiliation Switch Bug (the "Option Switch" bug) Disenfranchised Voters in Eight New Jersey Counties

340. On February 5, 2008, at least thirty-seven DREs in eight counties lost votes or allowed Republican or Democratic voters to vote in the primary of the other party. (Appel, Report, § 56.1, at 115.)[15] Professor Appel concluded that a single "option-switch bug," which he demonstrated on videotape and in Court, was the culprit. (Appel Test., 1/29 Trial Tr. at 165:22 to 169:10; Appel Report, § 56.1, at 115.)

341. The impact of this bug to the public is that voters are effectively prevented from voting in their own party primaries, which they have a right to do. Equally

[15] An OPRA (Open Public Records Act) request to all counties for copies of results report printouts that exhibited anomalies yielded the following results: Bergen (4 machines), Burlington (1), Camden (1), Cape May (4), Gloucester (2), Hudson (16), Ocean (1), Union (8). (Appel Report, § 56.2, at 115 n.103.)

disturbing, they are also permitted to vote in the opposite party's primary and have that vote counted. (Appel Test., 1/29 Trial Tr. at 157:14 to 158:2; 159:15-19; 161:1-12; Appel Report, § 56.22, at 121.)

342. In New Jersey, the law is clear that a voter can only vote in the primary of the party of which he or she is a registered member. N.J.S.A. § 19:23-45.

343. The usual practice is that a voter approaches a poll worker at a desk, countersigns his or her signature in the voting registry, and is handed a ticket called a "Voting Authority" by the poll worker. (Appel Test., 1/27 Trial Tr. at 158:20-22; Appel Report, § 29.1, at 75.) Then, the voter approaches another poll worker, the operator of the DRE, and hands the Voting Authority to that poll worker. (Appel Test., 1/27 Trial Tr. at 159:1-3.) The poll worker then activates the DRE for the voter by pressing a button, either 6 or 12, labeled with the appropriate party name, and then the Activate button.[16] (Appel Test., 1/29 Trial Tr. at 157:14-21.)

344. However, if the poll worker presses 6, then an incorrect button, such as the 7 button immediately next to the Activate button, then pushes the Activate button, the DRE will activate the party associated with button 12 instead. (Appel Test., 1/29 Trial Tr. at 157:22 to 158:2.) There is no external indication to the voter of which party slate is activated. (Appel Report, § 34.3, at 84.)

345. In the case of the Union County DREs which Professor Appel and his team examined, the DREs were set to use button 6 on the operator control panel to activate the Democratic Party slate of primary candidates, and button 12 for the

[16] Other counties may use different buttons for these same functions.

Republican Party slate, so the bug incorrectly activated the Republican primary for Democratic voters. (Appel Test., 1/29 Trial Tr. at 157:14-21; P-25.) Despite this, the DRE still counted the voter as having voted in the Democratic primary, but added 1 to the vote total of a Republican primary candidate. (Appel Test., 1/29 Trial Tr. at 161:6-13.) Other reports show similar misattribution of votes. (Ex. P-25.)

346. As a result, the Union County vote totals on this particular DRE were, for the Democrats: Obama 182, Clinton 179, for a total of 361. (Appel Test., 2/4 Trial Tr. at 30:7-10; Appel Report, § 56.11-13, at 118; Exs. P-25 and P-26.) However, the total number of voters listed as having voted in the Democratic primary was 362. (Id.) This means that there were more Democratic voters than there were Democratic votes. (Appel Test., 2/4 Trial Tr. at 34:5-8.) This should be impossible in a primary. The ballot definition file requires every voter to cast a vote for exactly one candidate in the primary election. Unless the voter chooses a candidate, pressing the "Cast Vote" button has no effect and is ignored by the DRE. (Appel Report, § 56.13, at 118.)

347. Another problem caused by the option switch bug in Union County was that while there were 61 total Republican votes, the Republican voter total is only 60. (Appel Test., 2/4 Trial Tr. at 32:23 to 33:12.) This means there are more Republican votes than Republican voters – which should be an impossibility. (Appel Test., 2/4 Trial Tr. at 32:23 to 33:17; Appel Report, § 56.11-13, at 118.)

348. In counties where button 6 was used to activate the Republican ballot and button 12 was used to activate the Democratic ballot, the results were reversed with

respect to party, but otherwise identical. (Appel Test., 2/4 Trial Tr. at 32:24 to 34:8; Appel Report, § 56.19, at 120.)

349. A software program should be written so that incorrect input either results in an error message or no action. (Appel Test., 1/29 Trial Tr. at 165:12-21.) For the Sequoia AVC Advantage 9.00H DRE to allow vote totals which could not possibly occur in reality and which are, on their face, inconsistent with themselves, is clearly unacceptable programming practice and constitutes a bug. (Appel Test., 1/29 Trial Tr. at 165:16-21.)

2. Sloppy User Interface Design in the Sequoia AVC Advantage 9.00H can Confuse Voters and Result in the Loss of Votes

350. Voters communicate their intent to the Sequoia AVC Advantage and receive feedback on whether their vote has been successfully cast through a number of buttons, LCD screens, and other devices, all of which are collectively called a user interface. (Appel Test., 1/27 Trial Tr. at 104:24 to 105:1; Appel Report, § 28.3, at 75.)

351. Sequoia's sloppy design practices have resulted in a number of defects in the user interface of the Sequoia AVC Advantage DRE, which can result in votes not being counted, allow poll workers to collude with voters to perpetrate vote fraud, and cause other problems. (Appel Test., 2/4 Trial Tr. at 72:5-11; Appel Report, § 28.3, at 75.)

352. As a result, voters can be disenfranchised either unintentionally or fraudulently. (Appel Report, § 28.4, at 75.)

3. AVC Advantage Falsely Indicates Votes Are Recorded, When They Are Not

353. When a voter attempts to cast votes when the DRE is not activated, the AVC Advantage gives multiple false indications that a vote is recorded:

- **The Advantage lights the X by each selected candidate button.**
- **It illuminates the Cast Vote button when pressed.**
- **It displays "VOTE RECORDED THANK YOU" on the LCD panel, just as if a vote had been cast.**

(Appel Test., 1/29 Trial Tr. at 183:9 to 185:3, Appel Report, § 30.1, at 79; Appel Test., 1/29 Trial Tr. at 177:24 to 178:4; DVD 1 Tape 1, at 17:30 to 18:14.)

354. This behavior could occur if a poll worker fails to press the Activate button before the voter enters the booth. (Appel Test., 1/29 Trial Tr. at 173:19 to 174:9; Appel Report, § 30.5, at 79.) The poll worker could fail to press the Activate button innocently, but a corrupt poll worker could also fail to press the Activate button as part of a vote-stealing scheme. (Appel Report, § 30.7, at 80.) The results in either case are the same; voters are disenfranchised. (DVD 1 Tape 1, at 18:34 to 19:55.)

355. This behavior is consistent with evidence of a 1% lost-vote rate in Pennsauken election district 6, Camden County, where there were 283 Democratic Voting-Authority stubs but only 279 or 280 votes cast. (Appel Report, § 30.4, at 79; Fig. 36, at 127.)

356. Even when no malicious poll workers are involved, votes will be lost and voters disenfranchised simply because of the extremely misleading feedback given by

the AVC Advantage's deeply flawed user interface. (Appel Test., 2/4 Trial Tr. at 69:23 to 70:16; Appel Report, § 30.7, at 80)

4. The AVC Advantage's User Interface is Flawed, Causing Voter Confusion and Disenfranchisement

357. Due to the primitive buttons-and-lights design of the AVC Advantage user interface, it is unable to communicate certain kinds of information to the user, leading it to give confusing feedback which makes it difficult for voters to determine if their votes have actually been cast, or falsely indicating that votes have been cast when they have not. (See generally Appel Test., 1/29 Trial Tr. at 176:3-20, 174:11-16; Appel Report, § 38.1, at 87.)

358. As a result of these easily avoidable mistakes, the AVC Advantage 9.00H is a deeply flawed DRE which makes under-votes, fraud, and other forms of disenfranchisement easy to commit, deliberately or inadvertently, and difficult to detect. (Appel Report, § 38.3, at 87.)

359. The behavior where the AVC Advantage DRE, when deactivated, lights a green X when a candidate's name is pressed, is very confusing user feedback and could very easily convince a voter that she had successfully cast a vote. (Appel Test., 1/29 Trial Tr. at 174:11-16; Appel Report, § 38.2, at 87.)

360. Dr. Shamos, Defendants' expert, agrees that this behavior is "confusing and risky." (Shamos Rebuttal, ¶ 112, at 25-26.) He even states that he personally reported this flaw in his 2006 evaluation of the AVC Advantage for Pennsylvania. (Id.) Sequoia has done absolutely nothing to remediate this glaring design flaw, which Dr. Shamos describes as a "misfeature." (Id.)

361. Similarly, the inadequacy of the privacy curtain in actually protecting voters from spying poll workers is obvious upon casual examination, and could have easily been avoided. (Appel Test., 1/29 Trial Tr. at 180:16-25; Appel Report, § 38.2, at 87.)

5. Sequoia has no Procedure for Dealing with the Problem of Fleeing Voters

362. Occasionally, voters will leave the voting booth before pressing the "Cast Vote" button. (Appel Test., 2/4 Trial Tr. at 73:19 to 74:16.) Sometimes, they will have pressed candidate buttons before fleeing, leaving their choices visible. (Appel Report, § J.8, at 152.) Whether they do this on purpose, or because they misunderstand the user interface of the DRE, this situation can cause a problem. (See generally Appel Report, § J, at 151-54.)

363. The Sequoia AVC Advantage Operator's Manual has no procedure for how to respond to this situation without violating the voter's privacy. (Appel Report, § J.9, at 152.)

364. There is no uniform, statewide policy on responding to this scenario, but the rules in at least one county for dealing with the "fleeing voter" scenario are cumbersome and time-consuming, and could cause delays at polling places or violate voter privacy. (Appel Report, §§ J.7-J.8, J.12, at 152-53.)

6. Pressing an Option Switch Deactivates the Advantage so that no Votes are Recorded

365. Similarly, if a poll worker operating an AVC Advantage inadvertently or deliberately presses an option-switch button, the Advantage is deactivated and records no votes. (Appel Test., 1/29 Trial Tr. at 185:17 to 186:8; Appel Report, § 31.1, at 80.) If, in a primary election, a poll worker activates a DRE for a

particular party by pressing that party's button (6 for Democratic and 12 for Republican) and then the Activate button, the poll worker can deactivate the DRE again by pressing the other party's button. (Appel Test., 1/29 Trial Tr. at 185:17 to 186:8; Appel Report, § 31.2, at 81; DVD 1 Tape 1, at 13:19 to 17:21.)

366. The result of deactivating the DRE in this way is that the DRE does not record votes, just as described in the previous section. (Appel Test., 1/29 Trial Tr. at 185:17 to 186:8; Appel Report, § 31.3, at 81.)

367. The DRE will make the usual chirping sound upon activation. However, there is no sound to indicate deactivation. (Appel Test., 1/29 Trial Tr. at 185:16 to 186:2; Appel Report, §§ 31.3-4, at 81.) A voter who is aware that the chirping sound indicates the DRE is activated and has heard the chirping sound has no audio cue that the DRE has actually been deactivated and is not recording votes. (Id.)

7. The Sound on Activation is not an Effective Signal for the Voter, Poll Workers, or Witnesses to Determine When Votes are being Cast

368. To prevent fraud, even early voting systems like ballot boxes had some protections against ballot stuffing, such as the presence of witnesses, the placement of the ballot box in a visible location, or a lever to open the box and insert a vote, which triggered a loud bell when votes were deposited. (Appel Report, § 32.3, at 82.)

369. Similarly, the old lever machines used in New Jersey through most of the twentieth century also made a loud sound when a vote was cast. (Appel Report, § 32.4, at 82.) As a visual cue, the lever machines also opened the curtain after a vote was cast, and closed the curtain when a poll worker activated the DRE. (Appel Report, § 32.4, at 82.) By contrast, the Sequoia AVC Advantage emits

only a soft chirping sound when the DRE is activated or when a vote is cast. (Appel Test., 1/27 Trial Tr. at 201:11-14; Appel Test., 1/29 Trial Tr. at 186:3-5; Appel Report, § 32.5, at 82.)

370. In the Sequoia AVC Advantage, if the operator presses the option switch after activating the DRE, the voter will hear the chirping sound indicating activation, even though the DRE is not activated and cannot record her vote. (Appel Test., 1/29 Trial Tr. at 185:13 to 186:2.)

371. The chirping sound is fairly faint, and a normal listener cannot hear it from a few feet away, or in a noisy environment, which many polling places are. (Appel Test., 2/4 Trial Tr. at 62:8-22; Appel Report, § 32.5, at 82.)

372. Additionally, unlike the lever machine with the curtain that opens and closes, the AVC Advantage does nothing visible which poll workers can watch for to see unusual behavior. (Appel Test., 1/29 Trial Tr. at 185:13 to 186:2; Appel Report, § 32.6, at 82.)

373. Further, the AVC Advantage makes exactly the same sound for activation and deactivation. When there are many AVC Advantage DREs in the same room, this gives little information even to a careful observer, as there is a constant din of chirping sounds throughout Election Day. (Appel Test., 2/4 Trial Tr. at 62:8-22; Appel Report, § 32.7, at 82.)

374. The AVC Advantage makes no sound at all if it is deactivated, leaving even someone who has carefully listened for each chirp unaware that the DRE has been deactivated. (Appel Test., 2/4 Trial Tr. at 62:8-22; Appel Report, § 32.8, at 83.)

8. The AVC Advantage's Lack of Feedback Leads Voters to Under-Vote

375. Professor David Kimball, a political scientist, did a study of the under-vote rate in the 2006 New Jersey general election. (Appel Report, § 33.3, at 83; David Kimball, Voting Equipment and Residual Votes on Ballot Initiatives: The 2006 Election in New Jersey, University of Missouri-St. Louis (Feb. 28, 2007.)) Kimball found a very high under-vote rate on public questions of around 29 percent, increasing for voters with lower incomes. (Id.)

376. Professor Appel found several possible technical explanations for this phenomenon, including the lack of a video screen or anything to alert the voter that she has forgotten to vote in certain contests. (Appel Test., 2/4 Trial Tr. at 74:7-16; Appel Report, § 33.5, at 83.) If this is accidental, the voter is inadvertently disenfranchised. (Appel Report, § 33.5, at 83; Appel Report, App. I, at 149-51 for more discussion of the lack of under-vote warnings.)[17]

9. Poll Worker Can See Who the Voter Votes For

377. The AVC Advantage has a privacy curtain, which is supposed to prevent poll workers and other observers from determining the voter's intent. (Appel Report, § 35.1, at 84.) However, the operator of the DRE, while standing at the operator panel, as intended, can peer through the slot and see the voter's finger as she casts votes. (Appel Test., 1/29 Trial Tr. at 180:15 to 181:1; Appel Report, § 35.5, at 85; Appel Report, Fig. 26, at 85; DVD 1 Tape 1 20:21 to 21:34.)

---

[17] Dr. Shamos, Defendants' expert, agrees that the AVC Advantage provides no adequate under-vote warning. (Testimony of Michael Shamos, March 25, 2009, Trial Tr. at 39:7-11.)

378. A dishonest poll worker familiar with the ballot, especially in a race with few candidates, would easily be able to tell which candidate a voter chose, or from the horizontal position of his finger, whether they voted a straight party ticket, and if so, for which party. (Appel Test., 1/29 Trial Tr. at 181:2-22; Appel Report, § 35.5, at 85.)

379. A corrupt poll worker could combine this fraud with the deactivation fraud described above to disenfranchise voters, by simply hitting the option-switch and deactivating the DRE as soon as he sees the voter's finger aiming toward a candidate the poll worker disfavors. (Appel Test., 1/29 Trial Tr. at 181:1-21; Appel Report, § 35.6, at 85.)

10. A Voter Cannot Undo a Write-in Vote, Violating FEC Guidelines

380. The FEC guidelines for DREs say: "A means for correcting a vote response should be readily available. For non-paper based systems, this should be built into the design of the system." (Appel Report, § 36.2, at 86; VVS 2002, App. C, § C.8(e).)

381. To cast a write-in vote on the AVC Advantage, the voter chooses a "candidate" marked "Personal Choice." (Appel Test., 1/27 Trial Tr. at 198:24-25; Appel Report, § 36.3, at 86.) Then, the voter types the name of her preferred write-in candidate on the small keyboard below the voter panel. (Appel Test., 1/27 Trial Tr. at 198:22-23.) The letters are displayed on the small LCD display below the voter panel. (Appel Test., 1/27 Trial Tr. at 199:2-14.) After typing the name, the voter may then type "Enter" to choose the candidate. (Id.)

382. Unlike casting a vote for a candidate on the ballot, where the voter can select and deselect a candidate by pressing the same button, which causes a green X to light

up or turn off next to the candidate's name, the voter is unable to deselect a write-in candidate if she changes her mind. (Appel Report, § 36.4, at 86.) This appears to violate the FEC guidelines. (Appel Report, § 36.5, at 86.)

S. The Lack of Statewide Protocols for Handling Results Reports and Results Cartridges, and the Poor Practices of Election Workers, Make Election Tampering Easy

1. Even Though the Paper Results Report Tape is Superior to the Results Cartridge for Election Results, Counties Rely on Easily Manipulated Results Cartridges for Election Results

383. When poll workers close the polls, a printer in the back of the Sequoia 9.00H DRE "automatically starts printing out a paper results report." (Appel Test., 1/27 Trial Tr. at 203:17 to 204:20, 167:14-24, 170:18-22, 171:12-14, 171:24 to 172:3; Appel Report, § 2.5.)

384. Results reports are produced from the vote totals stored in the internal memory of DREs "immediately when the polls close, in the presence of witnesses, [and are] signed by those witnesses[.]" (Appel Test., 1/28 Trial Tr. at 112:16-18; Appel Test., 2/4 Trial Tr. at 28:22 to 29:12, 52:2-19; Appel Report, § 41.2.)

385. The results report printout has a space for "poll workers to sign on the lines that they witness that this is the paper that came out of th[e] machine." (Appel Test., 1/27 Trial Tr. at 204:15-18; Appel Test., 2/9 Trial Tr. at 110:5-9.)

386. But, this printed record can be replaced with a fraudulent one. A dishonest poll worker can "reinsert a fraudulently doctored results cartridge into [a] voting machine to print phony results reports." (Appel Report, § 42.2 to 42.3.)

387. There is ample opportunity for such fraud. For example, the Middlesex County poll worker manual "explicitly recommends that poll workers perform other tasks at the very time [] results reports [are] printing." (Appel Report, § 42.5)

388. Additionally, Professor Appel testified to seeing Mercer County poll workers' casual treatment of results cartridges at the closing of the polls. (Appel Test., 1/27 Trial Tr. at 205:11-18, 206:8-23; Appel Test., 1/29 Trial Tr. at 100:16 to 101:25; Appel Test., 2/4 Trial Tr. at 26:2-20, 105:12 to 106:5, and 107:23 to 108:7.) Some poll workers pack paperwork, cartridges, and seals into canvas zipper bags and drive to municipal or county tabulation sites. (Appel Test., 1/27 Trial Tr. at 205:11-18; Appel Test., 1/29 Trial Tr. at 101:1-6.)

389. After the election, results cartridges transmit election results to WinEDS computers at municipal or county locations. (Appel Test., 1/27 Trial Tr. at 172:24 to 173:7; Appel Test., 1/28 Trial Tr. at 4:22 to 5:8, 6:9-19; Appel Test., 2/4 Trial Tr. at 19:22 to 20:10.) WinEDS converts data on results cartridges into summary reports. (Appel Test., 1/27 Trial Tr. at 211:21-25.)

390. There are ample opportunities for dishonest poll workers or election officials to write fraudulent data to results cartridges. (Appel Test., 1/29 Trial Tr. at 101:7-9, 103:21 to 104:3; Appel Report, § 40.6.)

391. When results cartridges are removed from DREs, they become immediately susceptible to physical and electronic manipulation. (Appel Test., 2/4 Trial Tr. at 55:17 to 56:18; Appel Report, § 40.1-40.2, § 40.8.)

392. Results cartridges can be manipulated while being transported to the municipal clerk. (See Appel Test., 1/29 Trial Tr. at 101:7-9; 103:21 to 104:3.)

393. Dishonest poll workers could use a simple program run from a personal computer to change votes on both the candidate total files and ballot image files. (Appel Test., 1/29 Trial Tr. at 96:18 to 97:2, 99:16-24; Appel Report, § 40.4.)

2. County Officials Rely on Results Cartridges for Official Election Reports

394. Even though results reports that are printed when the polls clos may reflect data manipulated by fraudulent firmware installed on a DRE, paper results reports printed immediately at the close of polls are superior to results cartridges as a source of election data. (Appel Test., 2/4 Trial Tr. at 26:7-20, 52:2-19; Appel Test., 1/28 Trial Tr. at 43:14-24; Appel Report, § 41.1-2.)

395. However, not all county clerks compare paper results reports from poll closings to result cartridges totals for each election district. (Appel Test., 1/28 Trial Tr. at 5:11-24.)

396. In Camden County, the Clerk apparently used election data from a "partially failed" results cartridge. (Appel Test., 1/28 Trial Tr. at 5:20-24; Appel Test., 2/4 Trial Tr. at 52:20 to 53:18; Appel Report, § 41.5, § 57.4.)

T. The Relationship Between Security, Reliability, and Accuracy

397. Professor Appel testified that as a general principle of computer security, paperless DRE machines are insecure and cannot be relied on. (Appel Test., 2/5 Trial Tr. at 56:22-24). If a voting system, such as the AVC Advantage, has security vulnerabilities that allow attackers to manipulate it and steal arbitrary numbers of votes, then we cannot rely upon it to count votes accurately. (Appel Test., 2/5 Trial Tr. at 54:10-15.) It can be as inaccurate to any extent an attacker desires. (Id.) Therefore, as a matter of computer science, a DRE which is insecure cannot be reliable or accurate. (Appel Test., 2/5 Trial Tr. at 54:15-16.)

398. By contrast, a DRE which is secure can be either accurate or inaccurate. (Appel Test., 2/5 Trial Tr. at 54:16-17.) For example, a DRE could be secure against attackers, yet count votes inaccurately. (Appel Test., 2/5 Trial Tr. at 18-19.)

Thus, it is possible for a DRE to be secure and accurate, or secure and inaccurate; but if it is insecure, it cannot, by definition, be accurate. (Appel Test., 2/5 Trial Tr. at 55:7-12.) If a DRE is inaccurate, then we cannot rely on it; and by definition it is unreliable. (Appel Test., 2/5 Trial Tr. at 55:14-19.)

399. To the extent that we can verify that an insecure machine has not been tampered with, it may be accurate or inaccurate in varying degrees. (Appel Test., 2/5 Trial Tr. at 56:2-4.) The Sequoia AVC Advantage 9.00H DRE, however, is a paperless DRE with no means by which voters or election officials can check the accuracy of votes, or recount them afterward to determine if the DRE has counted votes inaccurately. (Appel Test., 2/5 Trial Tr. at 56:19-24.)

400. The Advantage 9.00H DRE is insecure, and there are no reasonable means to remediate this insecurity. (Appel Test., 2/5 Trial Tr. at 57:2-7.)

U. There is a Safe Way to Use Computers to Count Votes

1. Voter-Verified Paper Ballots Ensure Secure and Accurate Elections

401. Professor Appel demonstrated many ways that DREs are unreliable and insecure, and can be made to cheat. There are ways to remediate these insecurities. Indeed, Professor Appel believes that it is possible to use computers to count votes. That is through software independent auditable systems. (See generally Appel Report, § 66, at 139-42.)

402. Software independence in electronic voting is the principle that it should be possible to verify vote totals independently of the computer program used to count them, if the results are in question. (Appel Test., 2/4 Trial Tr. at 100:4-20; Appel Report, § 66.1, at 139.)

403. Among experts in computer security who study voting systems, software independence is considered the superior means of ensuring electoral accuracy. (Appel Test., 4/14 Trial Tr. at 22:25 to 23:11.)

404. The only currently commercially available technology that achieves software independence is the voter-verified paper ballot. (Appel Test., 4/14 30:24 to 31:4; Appel Report, § 66.2, at 139.)

405. The scientific consensus in the computer security field concerning voting systems is that precinct-count optical scan is superior to DREs with attached printers, which are themselves superior to parallel testing (and all other theoretical testing methods proposed by Dr. Shamos) as a means of ensuring audit-ability and security. (Appel Test., 4/14 Trial Tr. at 24:5 to 26:21.)

406. Professor Appel testified that Dr. Shamos' proposed method of parallel testing would not reliably detect the presence of fraudulent firmware. (Appel Test., 4/14 Trial Tr. at 22:11-16.) This is because for any series of parallel tests, an attacker can devise a piece of fraudulent firmware which defeats those tests. (Appel Test., 4/14 Trial Tr. at 22:17-24.)

407. The consensus of scientific experts who study voting systems consider parallel testing an inferior method of establishing the integrity of elections. (Appel Test., 4/14 Trial Tr. at 22:25 to 23:6.) These experts consider software independence using voter-verified paper trails to be superior to parallel testing. (Appel Test., 4/14 Trial Tr. at 23:7-11.) Professor Appel personally consulted with the very experts who Dr. Shamos claimed supported the parallel testing, and they

uniformly believed parallel testing to be inferior to software independence in the form of a voter-verified paper ballot. (Appel Test., 4/14 Trial Tr. at 24:5-23.)

408. Further, Professor Appel consulted the Brennan Center for Justice report cited by Dr. Shamos in his testimony, of whom the principal investigator is Eric Lazarus. Dr. Shamos cited Eric Lazarus as supporting his position on parallel testing. (Appel Test., 4/14 Trial Tr. at 26:22 to 27:3.) Michael Waldman, also cited by Dr. Shamos in his testimony, is the Director of the Brennan Center for Justice. (Appel Test., 4/14 Trial Tr. at 27:4-7; P-75.)

409. This Brennan Center report, entitled "The Machinery of Democracy, Protecting Elections in an Electronic World," states explicitly: "The task force does not recommend parallel testing as a substitute for the use of voter-verified paper records with an automatic routine audit." (Appel Test., 4/14 Trial Tr. at 28:2-8.) This clearly contradicts the testimony of Dr. Shamos. (Appel Test., 4/14 Trial Tr. at 28:9-11.)

410. The Brennan Center report also clearly endorses Professor Appel's position that parallel testing does not create an independent record of voter's choices, and would lead to an "arms race" between defender and attacker, the ultimate result of which cannot be predicted. (Appel Test., 4/14 Trial Tr. at 28:12 to 29:12.)

411. Professor Appel testified that checkpointing, also proposed by Dr. Shamos, is not a reliable means of achieving software independence. (Appel Test., 4/14 Trial Tr. at 45:1-5.)

412. Further, nobody anywhere has actually tested checkpointing as a means of detecting fraudulent firmware. (Appel Test., 4/14 Trial Tr. at 45:5-8.)

413. From a computer security perspective, the method proposed by Dr. Shamos is easily evaded by fraudulent firmware. (Appel Test., 4/14 Trial Tr. at 45:9-22.) Since the method proposed by Dr. Shamos requires pressing a button on the front of the DRE when testing is to begin, the fraudulent firmware could simply detect that the DRE was in testing mode, and not cheat while testing was occurring. (Id.)

414. Finally, it is not even possible to do checkpointing on the Advantage 9.00H DRE. (Appel Test, 4/14 Trial Tr. at 45:23 to 47:7.) This is because the Advantage 9.00H DRE does not have the hardware necessary to perform the test. (Id.) The Advantage 9.00H DRE has neither the button on the front, nor the special kind of write-only media which checkpointing requires.[18] (Id.)

415. A voter-verified paper ballot is an individual paper record of every vote cast, seen and verified by the voter at the time the vote is cast, and saved in a ballot box or bag so that the paper ballots can be recounted by hand if suspicions arise as to the totals. (Appel Test., 4/14 Trial Tr. at 32:7-17; Appel Report, § 66.2, at 139.)

416. The New Jersey Legislature, in 2005, passed a law requiring voter-verified paper ballots. N.J.S.A. § 19:48-1(b)(1.)[19] Even when there is no suspicion of tampering, testing a small but statistically significant sample of all precincts by recounting them could ensure a high probability that the overall result was honest and that widespread fraud or error would be detected. (Appel Test., 4/14 Trial Tr.

---

[18] "Write-only" media is media which can only be written to. The contents cannot be erased. This is necessary for checkpointing to prevent fraudulent firmware from simply overwriting the legitimate test results to make it look as if the DRE passed.

[19] The State Legislature subsequently, in 2009, conditionally suspended these provisions until funds are available. N.J.S.A. § 19:48-1(b)(2.)

at 32:7-17; Appel Report, § 66.3, at 139-40.) Indeed, the New Jersey Legislature passed a law requiring exactly this kind of random audit. N.J.S.A. § 19:61-9 (requiring creation of independent audit team to use statistical science methods to ensure accuracy of elections).

417. The provisions of N.J.S.A. § 19:61-9 require hand-to-eye verification of paper ballots, which clearly presupposes the existence of such ballots. N.J.S.A. § 19:61-9(a.)

418. The existence of voter-verified paper ballots is not just the law. It is also a good idea. Because the modalities of fraud or error vary greatly between the counting of paper ballots and the behavior of computer software, each form of counting acts as a check on the other. (Appel Report, § 66.4, at 140.) An attacker would face great difficulty attempting to use the methods Professor Appel demonstrated to this Court to attack systems with voter-verified paper records. (Appel Report, § 66.4, at 140.)

2. Forms of Voter-Verified Paper Ballots

419. There are three commercially available forms of voter-verified paper ballots: hand counted paper ballots, optical-scan ballots counted by computer, and paper ballots printed by a printer attached to a DRE. (Appel Test., 4/14 Trial Tr. at 30:16 to 31:4; Appel Report, § 67.1, at 140.)

420. It is the overwhelming consensus of computer scientists who have studied voting technology that the most trustworthy, robust, and reliable form of voter-verified paper ballot is the precinct-count optical-scan ballot. (Appel Test., 2/4 Trial Tr. at 101:3-18, 102:3-24; Appel Test., 4/14 Trial Tr. at 32:5-17, 30:13 to 31:22; Appel Report, § 67.2, at 140.)

421. An optical-scan ballot is a paper ballot filled out by the voter, who either fills in an oval or connects an arrow with a pencil to the name of his chosen candidates or ballot questions. (Appel Report, § 67.3, at 140.)

422. There are two typical ways to count optical-scan ballots. The less favored method is to gather the ballots from many precincts to a central location at the end of the voting day and then count the ballots in bulk with a high speed scanning computer. (Appel Report, § 67.3, at 140; Appel Report, § 67.12, at 142.)

423. The preferred method is the precinct-count method, in which a person, usually the voter herself, places the completed ballot into an optical-scanning machine located in the polling place. (Appel Test., 2/4 Trial Tr. at 101:3-18, 102:3-24; Appel Test., 4/14 Trial Tr. at 32:5-17; Appel Report, § 67.3, at 140; § 67.12, at 142.)

424. The precinct-count method is favored for a number of reasons related to security and accuracy. These include:

- If the voter feeds an overvoted or otherwise invalid ballot into a precinct-count optical scan, the machine spits it back out with an informational message explaining the error, and the voter is offered an opportunity to correct it immediately, practically eliminating accidental overvoting.[20] (Appel Report, § 67.12(1), at 142.)
- Precinct-count optical-scanners deliver a total immediately upon the close of the polling place, while witnesses are still present, which ensures security, reliability, and a clean chain of custody. (Appel Report, § 67.12(2), at 142.)

[20] There is usually an override which allows a voter to cast the ballot anyway. (Appel Report, § 67.12 n.128, at 142.)

425. By comparison, central-count optical scanning systems require election workers to transport ballot boxes to a central location, introducing opportunities for unobserved manipulation, ballot box stuffing, and substitution of altered ballots. (Appel Report, § 67.12(2), at 142.) While optical-scanning systems are a computer-based, like DREs, and can similarly be hacked, when a paperless DRE is hacked, the game is over. There is no way to audit the results, as required by New Jersey law and by the New Jersey and U.S. Constitutions. By comparison, with precinct-count optical-scanning systems, there is a paper record of the election which can be compared against the computer tally. Each method of tallying can be used to check the accuracy of the other. (Appel Test., 4/14 Trial Tr. at 32:1-17.)

426. Optical-scan voting also has substantial advantages over DREs with paper-ballot printers, including the following:

- Using a paper ballot, voters actually personally examine and create the ballot which they present to the machine. While there is uncertainty about how closely people examine paper ballots printed by a DRE, there is no question that voters have examined an optical-scan ballot since they made the marks themselves. (Appel Test., 4/14 Trial Tr. at 31:5-14; Appel Report, § 67.6, at 141.)
- All voting machines can malfunction. When a DRE stops working, voters are completely unable to vote. However, if a precinct-count optical-scan machine breaks, voters can continue filling out paper ballots at the same rate of speed, saving them in a ballot box for counting later, after the machine is repaired or replaced. (Appel Test., 4/14 Trial Tr. at 32:7-17; Appel Report, § 67.7, at 141.)
- Only one voter at a time can use a DRE. When ballots are complicated or contain many candidates or ballot questions, this can greatly slow down the voting process. By comparison, multiple voters can fill out their paper ballots at the same time in, a booth containing nothing more than a flat surface and a pencil, costing virtually nothing. Then,

when the voters have finished filling out their ballots, they emerge and feed their ballots into the optical-scanner. (See Appel Test., 2/4 Trial Tr. at 21:13-22; Appel Report, § 67.8, at 141.)

- DREs with attached printers create a difficult situation for poll workers when a voter claims the printout doesn't match her vote. Either the DRE is malfunctioning or the voter is mistaken, or even lying. However, the poll worker has no way to figure out which is the case, since watching the voter cast her votes would invade the privacy of the voter. By comparison, there is no doubt about where the marks are on a paper ballot. The voter made those marks with a pencil herself. (Appel Test., 4/14 Trial Tr. at 31:5-14; Appel Report, § 67.10, at 141-42.)
- DREs, as Professor Appel has demonstrated repeatedly during the course of this trial, often have confusing and ambiguous user interfaces. By comparison, the use of paper and pencil are intuitively obvious to voters, and when the optical-scanner accurately reports their vote to them, they can be confident that their vote has been counted. (Appel Report, § 67.11, at 142.)

427. Professor Appel testified that according to scientific literature, the error rate of any voting machine used in an election should not be more than one percent. (Appel Test., 2/9 Trial Tr. at 114:4-9.) Professor Appel testified that there are no methods used in New Jersey to test the error rate of New Jersey's DREs. (Appel Test., 2/9 Trial Tr. at 114:10-13.) Professor Appel has conducted scientific research that tested the error rate of precinct-based optical scanners. (Appel Test., 2/9 Trial Tr. at 114:17 to 115:1.)

428. Professor Appel studied the error rate of precinct-based optical scanners by examining all of the data related to the total hand count of optically scanned paper ballots used in the 2008 Minnesota Senate race. (Appel Test., 2/9 Trial Tr. at 114:17 to 115:1.)

429. Professor Appel testified that the Minnesota Senate race was one of the best sources of scientific data on the error rates of precinct-based optical-scanners. (Appel Test., 2/9 Trial Tr. at 115:22 to 116:1.) He was able to conduct his research because all the scanned paper ballots were re-counted by hand under Minnesota Law. (Id.)

430. Professor Appel testified that he reviewed the written records of the Minnesota senatorial election that used precinct-based optical scanners. (Appel Test., 2/9 Trial Tr. at 23-25; 116:22 to 117:1.) Professor Appel reviewed the official spreadsheets provided by the Secretary of State of Minnesota of the precinct totals that were recounted by each precinct, as well as newspaper articles on disputed ballots. Professor Appel published a report of his findings. (Id.) (Optical-scan voting extremely accurate in Minnesota, Professor Andrew Appel 1/28/2008 Accessed 6/26/09 http://www.freedom-to-tinker.com/blog/appel/optical-scan-voting-extremely-accurate-minnesota.)

431. Professor Appel testified that the error rate of the precinct-based optical-scanners was one hundredth of one percent or one in 10,000 ballots. (Appel Test., 2/9 Trial Tr. at 116:22 to 117:2.) This means that the accuracy of the precinct-based optical scanners was 99.99%. (Appel Optical-scan voting extremely accurate in Minnesota.)

432. Precinct-count optical-scan systems are also the most cost-effective for software independence because precincts need fewer optical-scanning voting machines than DRE machines. Further, the cost of machine failure for optical-scanning machines is much lower. DRE failure can lead to long lines or even a total

shutdown of the polling place, driving away voters for the two hours or more it takes to send out a spare. While it is still a good idea to have two machines at each precinct in case of failure, even a failure of both optical-scanning machines would not shut down the polling place in the precinct-count optical-scan system. (See Appel Test., 2/4 Trial Tr. at 21:13-22; Appel Report, § 67.9, at 141.)

433. The overwhelming majority of computer scientists and other election technology experts have concluded that precinct-count optical-scan systems are the most trustworthy, robust, and cost-effective method of voting that is now available. Professor Appel recommends that New Jersey adopt precinct-count optical-scan technology. (Appel Test., 2/4 Trial Tr. at 101:3-18, 102:3-24; Appel Test., 4/14 Trial Tr. at 32:5-17; Appel Report, § 67.13, at 142.)

III. Testimony of Professor Edward Felten

434. Princeton University Professor Edward Felten holds a Bachelor's degree in Physics from the California Institute of Technology and a Master's degree and Ph.D. in Computer Science and Engineering from the University of Washington. (Testimony of Edward Felten ("Felten Test."), Feb. 10, 2009 Trial Tr. at 12:23 to 13:2.)

435. Professor Felten has taught at Princeton University for fifteen years. He is tenured. He is a professor in both the Computer Science Department and the Woodrow Wilson School of Public Affairs. Professor Felten is also the Director of Princeton's Center for Information Technology Policy, a cross-disciplinary institute devoted to studying the relationship between digital technologies and public policy. (Felten Test., 2/10 Trial Tr. at 13:3-17.)

436. Professor Felten has voted on the Sequoia AVC Advantage 9.00H DRE in Mercer County. (Felten Test., 2/10 Trial Tr. at 16:12-18.)

437. Professor Felten has also studied the Sequoia AVC Advantage in his laboratory at Princeton University, where he has performed security and reliability studies on those DREs. (Felten Test., 2/10 Trial Tr. at 16:25 to 17:5; 15:5.)

438. Since 2004, Professor Felten has observed and photographed himself in close proximity to unattended Sequoia DREs at polling locations in Princeton, New Jersey in advance of elections. (Felten Test., 2/10 Trial Tr. at 16:12-13, 17:9-12; see generally Exs. P-39, P-40, P-41, P-42, P-43, P-44, P-45.) Professor Felten has observed and photographed himself near DREs out of professional concern and because he is concerned, as a citizen, that the DREs are left unguarded. (Felten Test., 2/10 Trial Tr. at 27:16-21.)

439. The first time Professor Felten observed an unattended Sequoia AVC Advantage DRE at a polling place was in November 2004, one or two nights prior to the Presidential election. That evening, Professor Felten was en route to an event for his daughter at the LittleBrook Elementary School in Princeton. Professor Felten entered the unlocked main door of the school and noticed four Sequoia Advantage DREs left unattended in the entrance lobby. (Felten Test., 2/10 Trial Tr. at 17:18 to 18:12.)

440. The DREs were not stored under lock and key. Rather, they were left out in the open in a school building that was accessible by the public. No key or security badge was required to enter the hallway where the Sequoia DREs were located. (Felten Test., 2/10 Trial Tr. at 18:16-19.)

441. Since there was no security guarding the Sequoia Advantage DREs, Professor Felten was able to take a close look at the DREs. (Felten Test., 2/10 Trial Tr. at 18:16 to 19:1.)

442. While Professor Felten examined the Sequoia Advantage DREs, there was no one else present in the area to stop him or question his activities. As a result, Professor Felten was able to examine the machines uninterrupted. (Felten Test., 2/10 Trial Tr. at 21:10-18, 22:2-7.) There were no signs prohibiting his actions. (Felten Test., 2/10 Trial Tr. at 22:8-13.)

443. In November 2006, on the Saturday before Election Day, Professor Felten again saw unattended Sequoia Advantage DREs, this time at the Methodist Church in Princeton. (Felten Test., 2/10 Trial Tr. at 23:10-23.) In the basement of the church, in the social hall, Professor Felten found two unattended DREs. (Id.)

444. The church was open. Although people were gathering for an event in another part of the building, the social hall where the DREs were located, was empty. (Felten Test., 2/10 Trial Tr. at 24:1-4.)

445. A security badge or key was not needed to enter the building or the area in which the unattended DREs were located. (Felten Test., 2/10 Trial Tr. at 23:8-12.) As such, Professor Felten was again able to gain unfettered access to the unattended Sequoia Advantage DREs. (Felten Test., 2/10 Trial Tr. at 23:24 to 24:19.) Professor Felten documented his ability to gain unfettered access to the DREs by photographing himself next to them. (Felten Test., 2/10 Trial Tr. at 24:21-23; Ex. P-39.) No one stopped him or questioned why he was taking a photograph of the Sequoia DREs. (Felten Test., 2/10 Trial Tr. at 24:15-18, 26:16-19.)

446. In February 2008, on two occasions prior to the February 5 Super Tuesday election, Professor Felten viewed more Sequoia DREs unattended at polling locations. (Felten Test., 2/10 Trial Tr. at 27:22 to 28:8.)

447. First, on February 3, 2008 at around 5:00 p.m., Professor Felten viewed unattended DREs in the social hall of the Methodist Church where he was taking his daughter for a function. (Felten Test., 2/10 Trial Tr. at 30:22-23, 31:5-7, 28:18 to 29:4.) Professor Felten viewed the DREs in the social hall, the same place where he saw them in November 2006. (Felten Test., 2/10 Trial Tr. at 29:7-11.)

448. The main doors of the church were once again open and access to the Sequoia DREs was unfettered. (Felten Test., 2/10 Trial Tr. at 32:3-13.) No assistance of anyone with a key or security pass was required to access the church or basement

area where the DREs were located. (Felten Test., 2/10 Trial Tr. at 32:8-21.) No one was guarding the DREs; there were no signs prohibiting touching of the DREs. (Felten Test., 2/10 Trial Tr. at 32:23 to 33:6.)

449. Professor Felton again approached and examined the DREs to see if they looked in any way different from those he had seen before. (Felten Test., 2/10 Trial Tr. at 31:19-22.) Professor Felten also checked to see whether there were any security seals visible from the outside of the DREs. (Id.)

450. Professor Felten once again documented that the DREs were unprotected by taking a picture of himself next to the DREs. (Felten Test., 2/10 Trial Tr. at 29:14-19; Ex. P-40.)

451. Professor Felten was not stopped or questioned about his proximity to the DREs or why he was taking photographs of them. (Felten Test., 2/10 Trial Tr. at 32:23 to 33:6.)

452. On February 4, 2008, Professor Felten viewed four unguarded Sequoia Advantage DREs in the multi-purpose roon of the LittleBrook Elementary School. (Felten Test., 2/10 Trial Tr. at 33:7-17.) As with the other polling locations, Professor Felten was able to approach the DREs without confronting any security obstacles. (Felten Test., 2/10 Trial Tr. at 33:21-23.)

453. Professor Felton approached the Sequoia Advantage DREs, looked them over, and waited next to the DREs for about fifteen minutes to see if anyone would approach him. (Felten Test., 2/10 Trial Tr. at 35:7-18.) No one questioned why Professor Felten was near the DREs. (Felten Test., 2/10 Trial Tr. at 35:13-15.) Professor Felten did not observe anyone else in the vicinity of the DREs. (Felten

Test., 2/10 Trial Tr. at 35:15.) No signs were posted prohibiting anyone from touching the DREs. (Felten Test., 2/10 Trial Tr. at 35:16-21.)

454. Professor Felten once again documented that the DREs were left unattended by taking a photograph of the four AVC Advantage DREs. (Felten Test., 2/10 Trial Tr. at 33:19-21; Ex. P-41.)

455. Prior to the June 2008 Presidential primaries, Professor Felten purposefully sought out unattended voting machines in Princeton. (Felten Test., 2/10 Trial Tr. at 36:16-18.) Before, in previous elections, he inadvertently stumbled upon the unguarded DREs. (Felten Test., 2/10 Trial Tr. at 36:16-18.) Professor Felton viewed unattended Sequoia Advantage voting machines at five different locations. (Felten Test., 2/10 Trial Tr. at 35:22 to 36:10.) Those locations were:

- LittleBrook Elementary School in the multi-purpose room;
- The Methodist Church in Princeton;
- Princeton Township Hall in the entry foyer;
- Community Park Elementary School in the gym; and
- Jadwin Hall on the Princeton University Campus, in an entry hallway.

(Felten Test., 2/10 Trial Tr. at 36:24 to 37:10.)

456. Professor Felten viewed a total of eighteen unattended voting machines at those five locations. (Felten Test., 2/10 Trial Tr. at 37:11-13.)

457. Professor Felten saw the Sequoia DREs at the Princeton Methodist Church on the evening of Sunday, June 1, 2008, and all of the other DREs on Monday, June 2, prior to the June 3, 2008 election. (Felten Test., 2/10 Trial Tr. at 37:18-21.)

458. When Professor Felten visited the Princeton Methodist Church on Sunday evening, June 1, 2008, he did not need keys to enter the church. Professor Felten

was able to observe two DREs with ease. (Felten Test., 2/10 Trial Tr. at 28:3-8.) The two DREs were in a hallway adjacent to the social hall where Professor Felten had previously viewed unattended DREs on February 3, 2008. (Felten Test., 2/10 Trial Tr. at 38:20-19.)

459. Professor Felten approached the DREs and took a photograph of them without being stopped or asked about his activities. (Felten Test., 2/10 Trial Tr. at 38:20 to 39:4; Ex. P-45.)

460. The next day, on Monday, June 2, 2008, Professor Felten saw unattended Sequoia Advantage DREs at the Princeton Township Hall, the Community Park Elementary School, at Jadwin Hall on the Princeton University campus, and at the Little Brook Elementary School. (Felten Test., 2/10 Trial Tr. at 36:24 to 37:10.)

461. At four of the polling places where Professor Felten saw DREs on June 2, 2008, prominent signs, both outdoor and indoor, directed the public to the locations of the Sequoia AVC Advantage DREs. (Felten Test., 2/10 Trial Tr. at 46:20 to 47:13, 50:12-16.)

462. In three of the locations where Professor Felten had never been before, Township Hall, Community Park School and Jadwin Hall, there were prominent signs both inside and outside the buildings directing the public to the DREs. Professor Felten followed those signs to find the Sequoia Advantage DREs unattended. (Felten Test., 2/10 Trial Tr. at 47:14-19.)

463. Professor Felten took pictures of the DREs at all of the locations he visited, (Felten Test., 2/10 Trial Tr. at 40:3-12; Exs. P-42 (Jadwin Hall), P-43 (Little

Brook School), P-44 (Township Hall), and P-45 (Methodist church)), except for the Community Park School because the lighting was inadequate.

464. Between 7 and 8 p.m. on June 2, Professor Felten observed the DREs at Jadwin Hall, located on the west side of the Princeton campus, which is attached to a loading dock. (Felten Test., 2/10 Trial Tr. at 41:1-16.) Connecting the loading dock to Jadwin Hall was a glass wall. The DREs could be seen even before one entered the building. (Felten Test., 2/10 Trial Tr. at 41:17 to 42:6.)

465. Four Sequoia DREs were left unattended in the Little Brook School multi-purpose room. (Felten Test., 2/10 Trial Tr. at 42:7-12.)

466. At the Princeton Township Hall, Professor Felten viewed four unattended DREs in the entry foyer. No signs were in place prohibiting Professor Felten or anyone else from touching the DREs. Professor Felten took a picture of himself by the machines, with no other persons present to stop him from doing so. (Felten Test., 2/10 Trial Tr. at 43:4 to 44:4.)

467. Professor Felten did not need a key or a security badge to enter the buildings or the vicinity of any of the five different locations where he saw DREs unattended prior to the June 2008 election. (Felten Test., 2/10 Trial Tr. at 44:22 to 45:5.)

468. No alarms sounded when Professor Felten entered any of the five buildings where he saw unattended DREs prior to the June 2008 election. (Felten Test., 2/10 Trial Tr. at 47:20-23.) All of the buildings were unlocked and open. (Felten Test., 2/10 Trial Tr. at 47:23.)

469. Professor Felten was not asked about what he was doing at any of the five buildings where he saw unattended DREs prior to the June 2008 election. He was

able to closely examine each unattended DRE without issue. (Felten Test., 2/10 Trial Tr. at 45:6-11.)

470. Professor Felten was able to ascertain that all of the voting machines were Sequoia AVC Advantage DREs. (Felten Test., 2/10 Trial Tr. at 45:12-15.)

IV. Testimony of Plaintiffs' Witness Elisa Gentile

471. Ms. Gentile works for the Hudson County Superintendent of Elections as the voting machine warehouse supervisor. (Testimony of Elisa Gentile ("Gentile Test."), Feb. 23, 2009 Trial Tr. at 32:22 to 33:2.) She is a high school graduate. (Id. at 31:22.)

472. Ms. Gentile was originally listed as one of Defendants' witnesses. At trial, she testified as a witness on behalf of Plaintiffs.

473. After working for a number of years in a supermarket in Bayonne, New Jersey, Ms. Gentile accepted a position, in 1989, as a mechanic in Hudson County. (Gentile Test., 2/23 Trial Tr. at 32:7-16.) At that time, her work focused on maintaining and repairing lever voting machines made by Shoup. (Id. at 32:18-19.) Ms. Gentile was promoted to supervisor of the voting machine warehouse in approximately 1999. (Gentile Test., 2/23 Trial Tr. at 32:24 to 33:5.)

474. Since 2004, Hudson County has used Sequoia AVC Advantage DREs exclusively. (Gentile Test., 2/23 Trial Tr. at 34:1-6; 70:3-5.) Ms. Gentile received one week of technical training from Sequoia on the AVC Advantage DREs, and she participated in two WinEDS training classes. (Gentile Test., 2/23 Trial Tr. at 69:15 to 70:2.) The WinEDS training did not encompass issues related to security or "hackability" of the voting system. (Gentile Test., 2/23 Trial Tr. at 76:2-4.)

475. As supervisor of the voting machine warehouse, Ms. Gentile is responsible for maintaining the 600 Sequoia DREs used in Hudson County. (Gentile Test., 2/23 Trial Tr. at 33:16-24.)

476. She is also responsible for programming the DREs in advance of elections and transporting the DREs to and from polling places. (Id.)

477. Ms. Gentile supervises three permanent voting machine warehouse employees. (Gentile Test., 2/23 Trial Tr. at 34:24 to 35:3.) No other County employees work at the voting machine warehouse. (Id.) However, independent contractors from a company called Election Graphics are hired to perform certain tests prior to elections. (Gentile Test., 2/23 Trial Tr. at 48:1-5.)

478. The Hudson County voting machine warehouse is located at 86 Forest Street, in Jersey City, New Jersey. (Gentile Test., 2/23 Trial Tr. at 41:10-12.) 86 Forest Street is a three-story building. (Gentile Test., 2/23 Trial Tr. at 42:3-6.) Hudson County rents the second and third floors at 86 Forest Street from landlord Sal Casciano. (Gentile Test., 2/23 Trial Tr. at 41:18-23.) There is another tenant on the first floor that operates a music recording studio. (Gentile Test., 2/23 Trial Tr. at 42:16-17.)

479. Collectively, the second and third floors of 86 Forest Street occupy approximately 30,000 to 40,000 square feet of space – nearly the size of a football field. (Gentile Test., 2/23 Trial Tr. at 42:7-11, 42:25 to 43:3.) Hudson County stores 300 DREs on the second floor and 300 DREs on the third floor. (Gentile Test., 2/23 Trial Tr. at 43:6-11.) On each floor, the DREs are divided into rows of ten DREs with enough space between the rows to perform work on the machines. (Gentile Test., 2/23 Trial Tr. at 45:23 to 46:1-5.)

480. No security camera monitors the entrance to the second and third floors of 86 Forest Street. (Gentile Test., 2/23 Trial Tr. at 44:3-5.)

481. An alarm that is not tested protects the second and third floors of 86 Forest Street. (Gentile Test., 2/23 Trial Tr. at 44:6-12.) Arming the alarm requires entry of a four-digit security code. (Gentile Test., 2/23 Trial Tr. at 44:13-14.) Each employee at the voting machine warehouse has his or her own unique four-digit security code to arm the warehouse alarm; the codes have not changed since Ms. Gentile began working at the warehouse. (Gentile Test., 2/23 Trial Tr. at 44:19-24.)

482. Ms. Gentile and her three employees work from Monday through Friday, 8:30 a.m. to 4:30 p.m. (Gentile Test., 2/23 Trial Tr. at 45:6-11.) No security guards protect the warehouse during or after work hours. (Gentile Test., 2/23 Trial Tr. at 45:12-15.)

483. Ms. Gentile has no knowledge of whether her three employees have undergone a background check. (Gentile Test., 2/23 Trial Tr. at 40:25 to 41:2.)

484. To prepare the DREs for an election, Ms. Gentile and her employees charge and, if necessary, change the batteries of the voting machines, load the election-specific information onto results cartridges, and run diagnostic tests on the voting machines. (Gentile Test., 2/23 Trial Tr. at 46:6 to 47:25.) During much of the preparation for an election, the back doors of the DREs remain open and accessible both to voting warehouse staff and outside vendors performing work at the warehouse. (Gentile Test., 2/23 Trial Tr. at 50:20-23.)

485. Along with her employees, Ms. Gentile charges the batteries of the 600 voting machines every six to eight weeks. (Gentile Test., 2/23 Trial Tr. at 36:1-6.) The voting machines use a single 12-volt battery and four AA batteries. (Gentile

Test., 2/23 Trial Tr. at 37:8 to 38:4.) The AA batteries must also be changed. (Gentile Test., 2/23 Trial Tr. at 38:1-13.)

486. To change the four AA batteries, a voting machine warehouse employee must remove the metal back panel to put replacement batteries directly on the exposed motherboard. (Gentile Test., 2/23 Trial Tr. at 37:5 to 38:15.)

487. When changing the AA batteries, warehouse employees have access to open DREs. (Gentile Test., 2/23 Trial Tr. at 38:20-24.)

488. Ms. Gentile and the warehouse technicians conduct set-up diagnostics prior to each election. (Gentile Test., 2/23 Trial Tr. at 46:10-18.) Set-up diagnostics test only the physical workings of the DREs – the options switches on the operator panel, the polls open and polls closed switch, the on/off switch, and the write-in keyboard. (Id.)

489. Additionally, in preparation for an election, Ms. Gentile must burn specific ballot information onto results cartridges. Ms. Gentile obtains the ballot information from laptop computers that run the WinEDS operating system. (Gentile Test., 2/23 Trial Tr. at 54:1-15.) Ms. Gentile burns the information onto the results cartridges in the computer room of the Hudson County administration building. (Gentile Test., 2/23 Trial Tr. at 54:16-25.)

490. The laptops that Ms. Gentile uses to burn election-specific information onto the results cartridges are Internet-enabled and can receive an Internet signal during the burning process. (Gentile Test., 2/23 Trial Tr. at 56:16-23.) On occasion, Ms. Gentile has used a laptop at the voting machine warehouse, where there are

wireless Internet signals from another building in the vicinity. (Gentile Test., 2/23 Trial Tr. at 56:16 to 57:10.)

491. When the burning process is complete, Ms. Gentile and her employees transport the results cartridges back to the voting machine warehouse. (Gentile Test., 2/23 Trial Tr. at 57:13-17.)

492. Once the election-specific information has been loaded onto the results cartridges, Ms. Gentile and her employees place a cartridge into every DRE. (Gentile Test., 2/23 Trial Tr. at 57:13-20.) The DREs are then ready for the diagnostic Pre Logic Accuracy Test ("Pre-LAT"), which involves performing a mock vote for each candidate on the ballot on each DRE. (Gentile Test., 2/23 Trial Tr. at 47:17 to 48:24.)

493. Hudson County hires Elections Graphics, an outside vendor, to conduct Pre-LAT tests on all DREs. (Gentile Test., 2/23 Trial Tr. at 48:1-5.) Election Graphics usually sends the same group of employees to conduct the Pre-LAT tests on the DREs. (Gentile Test., 2/23 Trial Tr. at 49:18-24.) At times, however, Election Graphics sends someone with whom Ms. Gentile is unfamiliar. (Gentile Test., 2/23 Trial Tr. at 49:21-24.)

494. Neither Ms. Gentile nor her employees supervise the Election Graphics employees when they are conducting Pre-LAT tests at the voting machine warehouse. (Gentile Test., 2/23 Trial Tr. at 50:13-18.) The Election Graphics employees spread out in the large warehouse and at times are completely alone with the DREs. (Gentile Test., 2/23 Trial Tr. at 50:4-12.)

495. Ms. Gentile is unaware of any background checks that Election Graphics performs on its employees or that the County performs on Election Graphics employees. (Gentile Test., 2/23 Trial Tr. at 51:4-7.) No additional security is present at the voting machine warehouse when the Election Graphics employees are present. (Gentile Test., 2/23 Trial Tr. at 51:14-17.)

496. After Election Graphics performs the Pre-LAT tests, Ms. Gentile and her employees examine the results tapes corresponding with the Pre-LAT tests. (Gentile Test., 2/23 Trial Tr. at 51:18-25.) Provided the results are satisfactory, Ms. Gentile and her employees place a seal on the results cartridge in each voting machine. (Gentile Test., 2/23 Trial Tr. at 51:18-24.)

497. But, the Pre-LAT tests would not detect fraud because, in Hudson County, the Pre-LAT test involves casting one vote for each candidate for each contest and one vote for each public question on each DRE. (Gentile Test., 2/23 Trial Tr. at 48:17-24.)

498. Ms. Gentile and her employees then lock the back door of each DRE. (Gentile Test., 2/23 Trial Tr. at 52:2-4.) Each DRE has a key. (Gentile Test., 2/23 Trial Tr. at 52:20-21.) Ms. Gentile keeps duplicate copies of each key in the voting machine warehouse. (Gentile Test., 2/23 Trial Tr. at 52:24 to 53:4.)

499. When all voting machines have been locked, Ms. Gentile collects all the keys and places them in an envelope. (Gentile Test., 2/23 Trial Tr. at 52:2-4.)

500. Keys have been lost in the past. (Gentile Test., 2/23 Trial Tr. at 52:22-23.) When this happens Ms. Gentile and her employees make copies of the keys. (Gentile

Test., 2/23 Trial Tr. at 53:1-10.) It is easy to make copies of the DRE keys. (Id. at 52:17 to 53:20.)

501. Until recently, Ms. Gentile kept the keys in an unlocked cabinet in her office at the voting machine warehouse. (Gentile Test., 2/23 Trial Tr. at 53:11-18.) After her deposition in this case, however, Ms. Gentile placed a lock on the cabinet. (Gentile Test., 2/23 Trial Tr. at 53:14-18.)

502. No written procedures exist regarding the locking and unlocking of the back door of the voting machines. (Gentile Test., 2/23 Trial Tr. at 53:22-25.)

503. After locking the back door of the DREs, Ms. Gentile and her employees prepare to send the DREs to the approximately 245 polling locations in Hudson County. (Gentile Test., 2/23 Trial Tr. at 57:21 to 58:2.)

504. Penza Moving Company ("Penza"), another outside vendor, located in Jersey City, New Jersey, is responsible for transporting the Sequoia DREs to Hudson County polling locations. (Gentile Test., 2/23 Trial Tr. at 58:12-18.) To transport the DREs, Penza uses between three and four moving trucks with as many as four employees per truck. (Gentile Test., 2/23 Trial Tr. at 59:3-8.)

505. In most instances, one Penza employee drives the truck while at least one or two Penza employees remain in the rear of the truck alone with the DREs. (Gentile Test., 2/23 Trial Tr. at 59:9-19.) No member of the Hudson County voting machine warehouse staff accompanies the Penza movers during the transportation of the DREs. (Gentile Test., 2/23 Trial Tr. at 59:14-16.)

506. Although Penza tends to send the same group of employees to transport the DREs, that is not always the case. (Gentile Test., 2/23 Trial Tr. at 58:19 to 59:2.)

Penza has sent individuals to transport the DREs with whom Ms. Gentile is unfamiliar. (Gentile Test., 2/23 Trial Tr. at 58:19 to 59:2.)

507. Ms. Gentile is unaware of whether any background checks are performed on Penza's employees. (Gentile Test., 2/23 Trial Tr. at 59:20-22.) She does not know whether any Penza employee has a criminal record. (Gentile Test., 2/23 Trial Tr. at 60:1-3.) Ms. Gentile is unaware whether any Penza employee has a computer programming background. (Gentile Test., 2/23 Trial Tr. at 59:23-25.)

508. After the DREs are loaded onto Penza trucks and leave the warehouse, Ms. Gentile receives no official word from either Penza or a responsible party at the polling locations that the DREs have been delivered. (Gentile Test., 2/23 Trial Tr. at 61:9-11.) There is no way for Ms. Gentile to know whether the moving truck got delayed, took a detour, or failed to reach its destination. Ms. Gentile receives no indication whether the DREs reached a polling location in a timely manner. (Gentile Test., 2/23 Trial Tr. at 61:6-14.)

509. In Hudson County, no individual awaits delivery of the DREs before an election. (Gentile Test., 2/23 Trial Tr. at 61:12-14.)

510. Delivery of the DREs begins as early as a week before an election. (Gentile Test., 2/23 Trial Tr. at 61:15-22.) The DREs sit unattended at a polling location for as long as a week before an election. (Gentile Test., 2/23 Trial Tr. at 61:23-25.)

511. After the end of an election in Hudson County, the DREs remain at polling locations unattended for as long as one week before being transported back to the voting machine warehouse. (Gentile Test., 2/23 Trial Tr. at 62:10-12.)

V. Testimony of Daryl Mahoney

512. Daryl Mahoney is the Assistant Director of Voting Machines for Bergen County. (Testimony of Daryl Mahoney ("Mahoney Test."), Feb. 23, 2009 Trial Tr. at 80:10-15.) Mr. Mahoney works in the Bergen County voting machine warehouse. He is also a member of the Title 19 Voting Machine Certification Committee.

513. Mr. Mahoney is a high school graduate who majored in auto mechanics. (Mahoney Test., 2/23 Trial Tr. at 77:10-19, 78:3-8.) He was hired by Bergen County in 1993 as a voting machine mechanic for the lever voting machines made by Shoup. (Mahoney Test., 2/23 Trial Tr. at 79:6-11.)

514. Mr. Mahoney was originally listed as one of Defendants' witnesses, but Plaintiffs called Mr. Mahoney to testify on their behalf at trial.

515. Mr. Mahoney has no computer programming or computer software training. (Mahoney Test., 2/23 Trial Tr. at 84:8-21.)

516. Currently, Mr. Mahoney oversees the operation of the Bergen County voting machine warehouse along with the Director of Voting Machines. (Mahoney Test., 2/23 Trial Tr. at 80:10-15.)

517. Bergen County owns 1,200 Sequoia AVC Advantage DREs which are stored in the warehouse at 660 Gotham Parkway in Carlstadt, New Jersey. (Mahoney Test., 2/23 Trial Tr. at 80:16-20, 88:5-7.) According to Mr. Mahoney, there is a large sign on top of the warehouse that reads, in large print, "Bergen County Voting Machines." (Testimony of Daryl Mahoney ("Mahoney Test."), February 24, 2009 Trial Tr. at 48:4-19.)

518. At the voting machine warehouse, Bergen County employs ten full-time employees whom Mr. Mahoney supervises. (Mahoney Test., 2/23 Trial Tr. at 80:13-15, 89:8-10.) Temporary employees are employed during election time. (Mahoney Test., 2/23 Trial Tr. at 90:2-3.)

519. Criminal background checks are not performed on any of the employees of the Bergen County voting machine warehouse. (Mahoney Test., 2/23 Trial Tr. at 89:18-24, 91:10-14.)

520. To gain entrance into the warehouse, employees must use a code key to disarm an alarm and another code to unlock the door to enter the facility. (Mahoney Test., 2/23 Trial Tr. at 93:14 to 94:14.) The four-digit alarm code has remained the same for twelve years. (Mahoney Test., 2/23 Trial Tr. at 96:1-7.) All employees of the warehouse have the same three-digit code to unlock the door to the warehouse. The three-digit code has not been changed in at least five years. (Mahoney Test., 2/23 Trial Tr. at 96:21 to 97:12.)

521. In the warehouse, the DREs are organized alphabetically and are kept in the same order after every election. (Mahoney Test., 2/23 Trial Tr. at 98:12-22.) The DREs are marked externally to show the town, district, and polling location of each machine. (Mahoney Test., 2/23 Trial Tr. at 98:23 to 99:5.)

522. There is a key for every DRE. (Mahoney Test., 2/23 Trial Tr. at 99:6-7.) At certain times before each election throughout the year, the keys for the DREs remain with the DREs, and are not stored in a secure place. (Mahoney Test., 2/23 Trial Tr. at 99:8-16.)

523. Mechanics are responsible for the maintenance, repair, and pre-election set-up of the 1,200 Sequoia AVC Advantage DREs at the Bergen County warehouse. (Mahoney Test., 2/23 Trial Tr. at 100:4-6.) The mechanics can open the backs of the DREs at will and do not need authorization from anyone to gain access to the DREs. (Mahoney Test., 2/23 Trial Tr. at 100:7-16.)

524. Bergen County uses seven laptops to run the WinEDS system and to set up the DREs for elections. (Mahoney Test., 2/23 Trial Tr. at 110:22 to 111:5.) The laptops running the WinEDS system can be connected to the Internet. (Mahoney Test., 2/23 Trial Tr. at 111:20-22.)

525. In every Bergen County election, Sequoia is involved in many critical aspects of the voting preparation process. (Mahoney Test., 2/23 Trial Tr. at 112:2-20.) Sequoia prepares the ballot in Bergen County. (Mahoney Test., 2/23 Trial Tr. at 112:12-13.) Sequoia also downloads the ballot onto the laptops that run the WinEDS system. (Mahoney Test., 2/23 Trial Tr. at 112:14-16.) To download the ballot information onto the laptops that run WinEDS, Sequoia technicians use a jump drive. (Mahoney Test., 2/23 Trial Tr. at 112:2-8.)

526. Neither Mr. Mahoney, nor anyone else at the Bergen County voting machine warehouse, has ever analyzed the contents of the jump drive that Sequoia uses to load the ballot information onto the laptops. (Mahoney Test., 2/23 Trial Tr. at 114:11-16.) No one from the Bergen County warehouse has ever conducted tests on the laptops or the jump drives to determine if they have been corrupted with computer viruses. (Mahoney Test., 2/23 Trial Tr. at 114:17 to 115:19.) To Mr.

Mahoney's knowledge, no one has ever tested whether the results cartridges have been corrupted in any way. (Mahoney Test., 2/23 Trial Tr. at 115:20-23.)

527. At the Bergen County voting machine warehouse, the cartridges are kept stacked in lockable cabinets in a computer room, separate from the main office. (Mahoney Test., 2/23 Trial Tr. at 116:17 to 117:9.)

528. The mechanics at the warehouse load the results cartridges into the DREs. (Mahoney Test., 2/23 Trial Tr. at 118:2-5.) The backs of the DREs are kept unlocked. Keys to the DREs are left on top of each DRE during the ballot loading process. (Mahoney Test., 2/23 Trial Tr. at 118:10-22.)

529. In Bergen County, the warehouse mechanics perform the Pre-LAT tests prior to each election. (Mahoney Test., 2/23 Trial Tr. at 100:17-21.) Routinely, during the Pre-LAT test, the mechanics cast only one vote for each candidate on the ballot and each public question. (Mahoney Test., 2/23 Trial Tr. at 101:22-24.)

530. When the Bergen County Sequoia DREs were upgraded from version 5.0 to version 9.0H, (Mahoney Test., 2/23 Trial Tr. at 101:25 to 102:7), Election Graphics, an outside vendor, was hired to perform the upgrade. (Mahoney Test., 2/23 Trial Tr. at 102:12 to 103:20.) The upgrade took approximately four weeks to complete. (Mahoney Test., 2/23 Trial Tr. at 103:21-24.)

531. No background checks were conducted on Election Graphics employees before they came to the Bergen County voting machine warehouse to perform the upgrade on the Sequoia DREs. (Mahoney Test., 2/23 Trial Tr. at 103:2-5.)

532. While performing the upgrade, Election Graphics employees were given unsupervised access to the DREs. (Mahoney Test., 2/23 Trial Tr. at 103:2-12.)

533. Bergen County employs yet another contractor, Finkle Trucking ("Finkle"), to move the DREs back and forth from the warehouse to the polling locations. (Mahoney Test., 2/23 Trial Tr. at 104:7-11.) Over time, there has been employee turnaround at Finkle. (Mahoney Test., 2/23 Trial Tr. at 108:6-10.)

534. Mr. Mahoney does not know if Bergen County performs any background checks on the Finkle employees who are used to transport the DREs. (Mahoney Test., 2/23 Trial Tr. at 107:6-10.) Neither Mr. Mahoney nor anyone else at the warehouse conducts background checks on Finkle employees. (Mahoney Test., 2/23 Trial Tr. at 107:11-14.)

535. Mr. Mahoney does not know whether any of the Finkle employees have any background in computer science or computer programming. (Mahoney Test., 2/23 Trial Tr. at 107:19-22.)

536. Mr. Mahoney does not know whether any of the Finkle employees have criminal records or political party affiliations. (Mahoney Test., 2/23 Trial Tr. at 107:15-18, 107:23 to 108:1.)

537. Bergen County voting machines are delivered to polling locations anywhere from ten days to two weeks before an election. (Mahoney Test., 2/23 Trial Tr. at 108:20-25.) The DREs remain at polling locations after an election for the same period of time – about ten days to two weeks. (Mahoney Test., 2/23 Trial Tr. at 109:1-6.)

538. Bergen County warehouse employees do not accompany the Finkle trucks and the DREs during deliveries to and from the polling places. (Mahoney Test., 2/23 Trial Tr. at 109:19-22.)

539. Keys have been lost in the field in Bergen County. (Mahoney Test., 2/23 Trial Tr. at 118:23-25.) In fact, keys were lost in the November 2008 General Election. (Mahoney Test., 2/23 Trial Tr. at 119:11-23.) As of the date of Mr. Mahoney's testimony on February 23, 2009, however, locks for the DREs with lost keys had yet to be replaced. (Mahoney Test., 2/23 Trial Tr. at 119:17-23, 120:23 to 122:6.)

540. At the close of the polls, the head poll worker in a given polling location is responsible for transporting the results cartridges to the municipal clerk's office. (Mahoney Test., 2/23 Trial Tr. at 122:14-17.) The head poll worker is not accompanied by any Bergen County representative. (Mahoney Test., 2/23 Trial Tr. at 122:18-20.) From every municipality, the results cartridges are transported to the County Clerk's office on election night, where they are kept until the results of the election are certified. (Mahoney Test., 2/23 Trial Tr. at 123:10-21.) Once the election has been certified, the warehouse mechanics retrieve the results cartridges from the County Clerk's office. (Mahoney Test., 2/23 Trial Tr. at 123:25 to 124:4.)

541. Cartridges can be used interchangeably from DRE to DRE once the contents of the prior election have been erased. (Mahoney Test., 2/23 Trial Tr. at 124:5-6.)

A. Mr. Mahoney is a Member of the Title 19 Voting Machine Certification Committee

542. Mr. Mahoney is also a member of the Title 19 Voting Machine Certification Committee ("Title 19 Committee" or the "Committee"). (Mahoney Test., 2/23 Trial Tr. at 85:5-8.) The purpose of the Title 19 Committee is to evaluate voting equipment to determine if it meets the statutory requirements of Title 19. (Mahoney Test., 2/23 Trial Tr. at 125:12-16.) Mr. Mahoney has been a member

of the Title 19 Committee almost six years. (Mahoney Test., 2/23 Trial Tr. at 85:9-10.)

543. Mr. Mahoney did not know he was a member of the Title 19 Committee until he attended his second meeting. (Mahoney Test., 2/23 Trial Tr. at 85:20 to 86:5; 86:3-5.) No test was required of Mr. Mahoney to be on the Title 19 Committee. (Mahoney Test., 2/24 Trial Tr. at 11:2-4.) His work performance on the Committee has never been reviewed or evaluated. (Mahoney Test., 2/24 Trial Tr. at 11:8-11.)

544. Since Mr. Mahoney became a member of the Title 19 Committee, he has not received any training on computers or computer security. (Mahoney Test., 2/23 Trial Tr. at 87:17-23.)

545. The other members of the Title 19 Committee are Dick Woodbridge and John Fleming. (Mahoney Test., 2/23 Trial Tr. at 125:4-8.) Mr. Woodbridge is the chairman of the Committee. (Mahoney Test., 2/23 Trial Tr. at 125:6-7.)

546. No internal brochures, documents or checklists inform the Committee's interpretation of Title 19 or the testing and evaluation of the DREs. (Mahoney Test., 2/24 Trial Tr. at 12:7 to 13:6; see also Exs. P-46, P-47.)

547. The Title 19 Committee produces reports of its evaluations. (Mahoney Test., 2/23 Trial Tr. at 126:7-8.) All of the reports are authored by Mr. Woodbridge. (Mahoney Test., 2/23 Trial Tr. at 126:9-11.) Mr. Mahoney has never made a substantive change to a report authored by Mr. Woodbridge. (Mahoney Test., 2/23 Trial Tr. at 127:1-7.)

548. The Title 19 Committee has never consulted with any computer scientists or computer security experts in evaluating any DRE. (Mahoney Test., 2/23 Trial Tr. at 127:8-12.) Since Mr. Mahoney has been a member, the Title 19 Committee has never examined the software or the source code of any DRE. (Mahoney Test., 2/23 Trial Tr. at 127:17-25.)

549. The Title 19 Committee does not do any independent research to determine the accuracy of the vendors' claims about their voting systems. (Mahoney Test., 2/24 Trial Tr. at 13:12-20.)

550. The Title 19 Committee does not do any research to learn whether or not a particular DRE has been rejected by another state. (Mahoney Test., 2/24 Trial Tr. at 14:1-6.)

551. Mr. Mahoney was not aware of any requirement to retest a DRE after a certain number of years. (Mahoney Test., 2/24 Trial Tr. at 14:7-10.)

552. Exhibits P-46 and P-47, the provisions of Title 19 that the Committee uses to evaluate DREs, do not contain information about testing electronic DREs. (Mahoney Test., 2/24 Trial Tr. at 14:11-15.)

553. Mr. Mahoney testified that in March 2005, the Title 19 Committee was presented with a full software upgrade for the WinEDS system for use with the Sequoia AVC Advantage. (Mahoney Test., 2/24 Trial Tr. at 14:17 to 15:22; 19:6-25.) The new version was described as an "upgraded software system with additional enhancements." (Ex. P-48 at 1.) The upgrade included changes to "application commands that query the database" and affected both the "ballot management

portion of the software" and the "reporting module" in the application. (Ex. P-48 at 5-6.)

554. The certification hearing for this software upgrade lasted only 45 minutes. (Mahoney Test., 2/24 Trial Tr. at 20:6-13.) The Committee did not perform a full certification review. (Mahoney Test., 2/24 Trial Tr. at 21:19-23.) Instead, Mr. Woodbridge asked a Sequoia representative whether the software changes would impair the accuracy, efficiency or ability of the Sequoia AVC Advantage to meet the requirement of the statute. (Mahoney Test., 2/24 Trial Tr. at 20:20-25.) The Sequoia employee, Mr. McIntyre, responded that the new software meets the statutory criteria of 19:53A-4 and would provide enhancements and improvements to the system. (Mahoney Test., 2/24 Trial Tr. at 21:13-18.) Based on the representations made by Sequoia, the Title 19 Committee determined that a full recertification hearing was not necessary for the software upgrade. (Mahoney Test., 2/24 Trial Tr. at 21:19-23.)

555. During the certification hearing for this software upgrade, no one from the Committee analyzed the new software for accuracy or security or conducted any tests to determine the existence of any programming bugs in the new software system. (Mahoney Test., 2/24 Trial Tr. at 22:8-25.) Nor did the Committee review or apply the requirements of Title 19 as found in Exhibits P-46 or P-47. (Mahoney Test., 2/24 Trial Tr. at 25:21-24.)

556. Before issuing a letter recommending the Sequoia software upgrade be certified, no one from the Title 19 Committee consulted with any computer scientists or computer security experts. (Mahoney Test., 2/24 Trial Tr. at 23:1-4.)

557. On or about September 29, 2006, the Title 19 Committee again evaluated the WinEDS system. (Mahoney Test., 2/24 Trial Tr. at 26:14 to 27:23.) Because the Committee concluded that the changes to the WinEDS system involved an upgrade of the software, the Committee determined that it did not need to conduct a full recertification hearing. (Mahoney Test., 2/24 Trial Tr. at 29:16-20, 31:5-8.) The Committee identified only four of eighteen new items listed for the WinEDS system "as being changes relevant to the State of New Jersey," and the other items were "not relevant to the hearing." The Title 19 Committee concluded the WinEDS changes were improvements, even though "the new software and system" included additional functionality with respect to the security of the cartridges and the ability to create election cartridges faster. (Ex. P-50, at 2.)

558. Despite changes to the WinEDS software, no one on the Title 19 Committee conducted any tests or examined the source code or consulted with computer scientists or computer security experts. (Mahoney Test., 2/24 Trial Tr. at 31:5-16.)

559. Moreover, despite knowing that the WinEDS system connects to the Internet, (Mahoney Test., 2/24 Trial Tr. at 31:17 to 32:20), and well-aware that the Internet poses significant insecurity, particularly with regard to hacking, (Mahoney Test., 2/24 Trial Tr. at 32:21 to 33:3), Mr. Mahoney voiced no formal opposition to the certification of the WinEDS system. (Mahoney Test., 2/24 Trial Tr. at 33:3, 33:8-14.) Nobody else did either. (Id.)

560. Mr. Mahoney has never read reports from independent testing authorities ("ITA") from start to finish. (Mahoney Test., 2/24 Trial Tr. at 34:24 to 35:3.) He does not

completely understand ITA reports because they contain technical information. (Mahoney Test., 2/24 Trial Tr. at 35:4-8.)

561. After learning that Ciber Laboratories had been de-certified as an ITA, the Title 19 Committee did not meet to discuss the impact of the Ciber de-certification and whether any New Jersey voting systems that were tested by Ciber should be re-evaluated by the Committee. (Mahoney Test., 2/24 Trial Tr. at 36:12-17.)

562. Four voting machines in Bergen County experienced the option switch bug in the February 5, 2008 Presidential primary election. (Mahoney Test., 2/24 Trial Tr. at 36:18 to 38:25, 40:3-8.) However, Mr. Mahoney never called the other members of the Title 19 Committee to discuss the problem. (Mahoney Test., 2/24 Trial Tr. at 40:9-12.) The Title 19 Committee never met to discuss the option switch bug that caused the problems in the February 2008 Presidential primary. (Mahoney Test., 2/24 Trial Tr. at 40:13-22, 41:4-6.) Indeed, the Title 19 Committee took no corrective measures and never sought an explanation from Sequoia about what happened during the February 2008 Presidential primary. (Mahoney Test., 2/24 Trial Tr. at 40:13-18.)

563. As of the time of his trial testimony, on February 24, 2009, fully one-year later, Mr. Mahoney still did not know what caused the switching of votes in the February 2008 Presidential primary. (Mahoney Test., 2/24 Trial Tr. at 41:1-3.)

VI. Testimony of Paula Sollami-Covello

564. Paula Sollami-Covello is the Mercer County Clerk. (Testimony of Paula Sollami-Covello ("Sollami-Covello Test."), February 24, 2009 Trial Tr. at 55:16, 57:13-14.)

565. As Mercer County Clerk, Ms. Sollami-Covello supervises a staff of thirty-seven employees, some of whom oversee the elections in Mercer County. (Id. at 58:14-17.) The election staff usually consists of two full-time employees. (Id.)

566. The elections department is responsible for the entire election process. (Id. at 59:9-15.) The department responsibilities include, but are not limited to, printing sample and actual ballots, determining ballot formatting; issuing absentee ballots; advertising the various ways people can vote; tabulating election results, and verifying elections. (Testimony of Paula Sollami-Covello ("Sollami-Covello Test."), February 26, 2009 Trial Tr. at 55:9-18; Sollami-Covello Test., 2/24 Trial Tr. at 57:20, 59:15-25, 60:1-4.)

567. Mercer County uses over 500 Sequoia AVC Advantage 9.00H DREs for its elections. (Sollami-Covello Test., 2/24 Trial Tr. at 60:11-14.)

568. The Sequoia Advantage DREs record votes on results cartridges that are approximately the size of a VHS tape. (Sollami-Covello Test., 2/24 Trial Tr. at 62:10.)

569. The vote total is also recorded on paper tape readouts in the back of the DREs. (Sollami-Covello Test., 2/24 Trial Tr. at 64:13-15.)

570. On election night, after the close of the polls, each cartridge is sealed in a blue canvas envelope while the tape readout is placed in a front pouch of the canvas envelope. (Sollami-Covello Test., 2/24 Trial Tr. at 65:20-24.) These canvas

envelopes are signed by the board worker and transmitted to the municipal clerk's office. (Sollami-Covello Test., 2/24 Trial Tr. at 66:1-3, 61:5-7.)

571. The Mercer County Clerk's office retrieves the DRE results cartridges from each municipal clerk. (Sollami-Covello Test., 2/24 Trial Tr. at 61:6-7.)

572. At the Mercer County Clerk's office, three to four election officials are each given cartridge readers. (Sollami-Covello Test., 2/24 Trial Tr. at 61:9-11.)

573. Results cartridges are inserted into the cartridge readers which are connected to computers. (Sollami-Covello Test., 2/24 Trial Tr. at 61:12-13.) When a cartridge is in the cartridge reader, and the reader is connected to a computer, the computer displays the vote tallies registered on the inserted cartridge. (Sollami-Covello Test., 2/24 Trial Tr. at 62:10-14.)

574. WinEDS software is used to read cartridges. WinEDS is provided by Sequoia. (Sollami-Covello Test., 2/24 Trial Tr. at 62:17-19.)

575. Mercer County uses desktop personal computers to read the results cartridges. (Sollami-Covello Test., 2/24 Trial Tr. at 63:4-7.)

576. Each computer is also used for every day purposes. (Sollami-Covello Test., 2/24 Trial Tr. at 63:23-25.)

577. Each computer is also connected to the Internet. (Sollami-Covello Test., 2/24 Trial Tr. at 87:15-17.)

578. On election night, Ms. Sollami-Covello takes no action to verify that the computers with attached cartridge readers are disconnected from the Internet. (Sollami-Covello Test., 2/24 Trial Tr. at 91:15-21.)

579. On election night, Ms. Sollami-Covello's staff posts on the Internet the unofficial results gleaned from the cartridges. (Sollami-Covello Test., 2/24 Trial Tr. at 65:2-5.)

580. After the vote totals are gleaned from the cartridges, the results cartridges are returned to the Mercer County Clerk's office. (Sollami-Covello Test., 2/24 Trial Tr. at 61:21-22.) To access any stored cartridge, in the event that it needs to be re-read, several witnesses must be present. (Sollami-Covello Test., 2/24 Trial Tr. at 61:22-25, 62:1.) The cartridges remain in storage for ten to fourteen days after the election. (Sollami-Covello Test., 2/24 Trial Tr. at 62:1-3.)

581. After the unofficial results from the cartridges are posted on the Internet on election night, Ms. Sollami-Covello's staff has until the following Monday to verify and certify the official election results according to State law. (Sollami-Covello Test., 2/24 Trial Tr. at 64:9-11.)

582. Verification involves comparing the readout tapes from the DREs with the tallies from the cartridges. (Sollami-Covello Test., 2/24 Trial Tr. at 64:13-17.) Ms. Sollami-Covello's staff ensures that the numbers listed on the tapes match those recorded on the cartridges. (Id.)

583. After certification and verification, the cartridges are returned to the warehouse. (Sollami-Covello Test., 2/24 Trial Tr. at 62:4-5.) At the warehouse, the cartridges are cleared so they can be reused. (Sollami-Covello Test., 2/24 Trial Tr. at 62:5-7.)

584. The warehouse computers run WinEDS. (Sollami-Covello Test., 2/24 Trial Tr. at 64:4-6.)

585. Mercer County experienced problems with its Sequoia DREs in the February 5, 2008 Presidential primary election. (Sollami-Covello Test., 2/24 Trial Tr. at 66:4-16.)

586. Two days after the February 5, 2008 Presidential primary election, Ms. Sollami-Covello was alerted by the Union County Clerk, Joanne Rajoppi, to the possibility of a problem with Sequoia DREs. (Sollami-Covello Test., 2/24 Trial Tr. at 71:2-6.)

587. At Ms. Rajoppi's request, Ms. Sollami-Covello inspected the readout tapes from the Sequoia DREs. (Sollami-Covello Test., 2/26 Trial Tr. at 19:17-20; Sollami-Covello Test., 2/24 Trial Tr. at 67:2-3, 70:1.) Ms. Sollami-Covello's office compared the number of votes cast with the option switch totals, which register the number of voters. (Sollami-Covello Test., 2/26 Trial Tr. at 19:17-20; Sollami-Covello Test., 2/24 Trial Tr. at 67:2-3, 70:1.)

588. On the readout tape, option switch totals reflect the total numbers of registered voters who voted on a DRE and the party ballot they used. (Sollami-Covello Test., 2/24 Trial Tr. at 67:2-8.)

589. By law, in a primary election, a registered Democrat or Republican voter can only vote for the candidates running in the voter's party. N.J.S.A. 19:23-45. Thus, in a primary election, Democrats must vote for Democratic candidates and Republicans for Republican candidates.

590. For the February 5, 2008 Presidential primary, Mercer County had different results on readout tapes and cartridges for thirty Sequoia DREs. (Sollami-Covello Test., 2/24 Trial Tr. at 71:12-13.)

591. On thirty DREs, there were more votes than voters. (Sollami-Covello Test., 2/24 Trial Tr. at 67:13-16.)

592. In all but three cases, the number of over-votes for one party equaled the under-votes for the other party. (Sollami-Covello Test., 2/26 Trial Tr. at 6:6-15, 9:2.)

593. This means that a voter who was a registered Republican had no choice other than to vote in the Democratic primary (or vice versa). (See id. at 6:12-15.)

594. It is clear that some Democrats who were presented with a Republican ballot, attempted to vote for a Democratic candidate. Democrats who were presented with the Republican party ballot because of the option switch bug attempted to cast write-in votes for Hillary Clinton in the Republican primary. (Sollami-Covello Test., 2/26 Trial Tr. at 30:25-31:12.)

595. These write-in votes were not counted, because by law, one can only vote in the primary of the party of which one is registered.

596. In most cases, there was no explanation for how under-votes and over-votes were allocated by Mercer County's Sequoia DREs. (Sollami-Covello Test., 2/26 Trial Tr. at 18:8-20.)

597. Despite these problems, Ms. Sollami-Covello certified the official results using the votes recorded by the Sequoia DREs and ignoring the number of voters reported by the Sequoia DREs. (Sollami-Covello Test., 2/24 Trial Tr. at 79:15-17.)

598. Ms. Sollami-Covello did not consult the voter registration books to resolve the discrepancies. (Sollami-Covello Test., 2/24 Trial Tr. at 80:19-24.)

599. After observing the under-vote/over-vote problem on many DREs in Mercer County, Ms. Sollami-Covello reported the findings to Ms. Rajoppi. (Sollami-Covello Test., 2/24 Trial Tr. at 71:19-20.)

600. Ms. Sollami-Covello contacted the Mercer County Superintendent of Elections via e-mail and traditional mail to report the problem and request an investigation. (Sollami-Covello Test., 2/24 Trial Tr.at 72:1-2.) Copies of the letter went to Arthur Sypek, Mercer County counsel; Dominic Magnolo, chair of the Board of Elections, Mercer County; Marge Caldwell Wilson, the vice chair of the Board of Elections, Mercer County; Donna Kelly, the Deputy Attorney General in charge of elections; Rush Holt, Congressman, 12th Congressional District; Brian Hughes, the Mercer County Executive; and Lucy Walter, the chairman of the Mercer County Freeholder Board. (Sollami-Covello Test., 2/24 Trial Tr. at 73:19-25, 74:1-3.)

601. The Attorney General's office did not respond to Ms. Sollami-Covello. (Sollami-Covello Test., 2/24 Trial Tr. at 75:24-25, 76:1.)

602. The Superintendent of Elections never contacted Ms. Sollami-Covello to investigate the problem. (Sollami-Covello Test., 2/24 Trial Tr. at 82:19-21.)

603. Ms. Sollami-Covello also contacted Joe McIntyre at Sequoia to report the problem. (Sollami-Covello Test., 2/24 Trial Tr. at 74:18-21.) Sequoia responded only with a press release which attempted to explain the supposed cause of the error. (Sollami-Covello Test., 2/24 Trial Tr. at 76:2-8.)

VII. Testimony of Joanne Rajoppi

A. Ms. Rajoppi's Extensive Background in Public Service in New Jersey

604. Ms. Rajoppi is the Union County Clerk. (Testimony of Joanne Rajoppi ("Rajoppi Test."), February 26, 2009 Trial Tr. at 36:15-16.) There are over 300,000 registered voters in Union County. (Id. at 104:15-16.)

605. The office of County Clerk is an elected, constitutional office; Ms. Rajoppi has served in that position for three five-year terms thus far. (Rajoppi Test., 2/26 Trial Tr. at 37:9-11.)

606. Prior to her first election to the office of Union County Clerk, Ms. Rajoppi held a variety of elected offices, including Union County Register of Deeds and Mortgages, Union County Freeholder (Chair); Mayor of Springfield, New Jersey, and Council Person of Springfield, New Jersey. She has also served on her local Board of Education. (Rajoppi Test., 2/26 Trial Tr. at 37:12 to 38:4.)

607. Ms. Rajoppi is past-President and current member of the Constitutional Officers Association of New Jersey. This educational and legislative advocacy organization is made up of constitutional officers including clerks, surrogates and sheriffs. Through the Constitutional Officers Association, Ms. Rajoppi shares information with other County Clerks throughout the State regarding election-related issues. The organization also holds educational conferences and seminars. (Rajoppi Test., 2/26 Trial Tr. at 59:5 to 60:6.)

608. Ms. Rajoppi is also the Director of the Clerks' Division of the International Association of Clerks, Recorders, Election Officials, and Treasurers ("IACREOT"). In that role, she heads up all of the Clerks in the Association. (Rajoppi Test., 2/26 Trial Tr. at 60:11-23.)

609. Ms. Rajoppi holds a Master's Degree in Public Administration (M.P.A) from Seton Hall University, which she obtained in 1988. (Rajoppi Test., 2/26 Trial Tr. at 34:11-19.)

B. Ms. Rajoppi's Election Administration Duties

610. Union County uses the Sequoia AVC Advantage DREs, and has used these DRE since 1998. (Rajoppi Test., 2/26 Trial Tr. at 55:4-10.)

611. Ms. Rajoppi's responsibilities with regard to administering elections in Union County are multiple and diverse. (Rajoppi Test., 2/26 Trial Tr. at 38:24 to 39:5.).

612. Prior to a given election, Ms. Rajoppi's duties include the following:

- Ms. Rajoppi and her staff accept, review and approve petitions for county office. (Rajoppi Test., 2/26 Trial Tr. at 39:5-6.)
- If necessary, Ms. Rajoppi and her staff have a drawing to determine candidate placement on the Election Day ballot. (Rajoppi Test., 2/26 Trial Tr. at 39:9-10.)
- Ms. Rajoppi and her staff design and format the ballot which is ultimately affixed to the DRE. (Rajoppi Test., 2/26 Trial Tr. at 39:10-12.)
- Once the ballots are printed and delivered by hand from the printer to the voting machine warehouse, Ms. Rajoppi must inspect each and every one of Union County's DREs with the ballot affixed, to make sure that each is correct. (Rajoppi Test., 2/26 Trial Tr. at 39:24 to 40:4, 58:1-3.)
- Additionally, Ms. Rajoppi and her staff design the ballot for absentee, provisional, overseas, and military voters. (Rajoppi Test., 2/26 Trial Tr. at 39:13-15.) Moreover, in seventeen of the twenty-one towns in Union County, Ms. Rajoppi and her staff are obligated by federal law to produce Spanish ballots. (Rajoppi Test., 2/26 Trial Tr. at 39:17-21.)
- Ms. Rajoppi and her staff are responsible for sending out sample ballots to every registered voter in Union County, for sending out overseas ballots, and for sending out absentee ballots, (which also entails a verification process

to determine whether the absentee voters are truly registered.) (Rajoppi Test., 2/26 Trial Tr. at 40:5-13.)

613. On Election Day, Ms. Rajoppi's office is open for anyone who needs to go to Court for an election-related problem, such as when a voter's name does not appear in the poll book. (Rajoppi Test., 2/26 Trial Tr. at 40:19-23.)

614. Ms. Rajoppi notes that her "real work begins" after the polls have closed. (Rajoppi Test., 2/26 Trial Tr. at 40:24-25.) As the Union County Clerk, Ms. Rajoppi is charged with collecting the vote totals from the results cartridges within Union County's DREs, and certifying the election results. (Rajoppi Test., 2/26 Trial Tr. at 41:4-10.

C. The Tallying of the Vote and Certification of Elections in Union County

615. At the close of an election, all of Union County's results cartridges are ultimately transported to the Union County Clerk's office by members of the Sheriff's office. (Rajoppi Test., 2/26 Trial Tr. at 51:8-12.) Some of these results cartridges are read once they are arrive at the County Clerk's Office. (Rajoppi Test., 2/26 Trial Tr. at 45:6-7). The remainder of the results cartridges are read at one of Ms. Rajoppi's four satellite offices within Union County, prior to being transported to the County Clerk's office. (Rajoppi Test., 2/26 Trial Tr. at 41:1-7.)

616. The satellite offices are each equipped with a device called a cartridge reader, and a laptop that runs the WinEDS program; the laptop is used for no purpose other than elections. (Rajoppi Test., 2/26 Trial Tr. at 47:9 to 48:5.) The cartridge reader downloads the results from each cartridge onto the WinEDS laptop. (Rajoppi Test., 2/26 Trial Tr. at 48:18-25.)

617. The vote totals from the cartridges read at the satellite offices – which have been downloaded onto the WinEDS laptops – are transmitted to Ms. Rajoppi's office by way of a "TI line," which is a high-speed Internet line dedicated to this purpose. (Rajoppi Test., 2/26 Trial Tr. at 41:6-19, 49:19-20.) The vote totals are transmitted in an email format. (Rajoppi Test., 2/26 Trial Tr. at 49:10-11.)

618. During the evening of Election Day, once all of the results cartridges have been read and Ms. Rajoppi has received all of the vote totals from the various satellite offices, the election results are run through the WinEDS program and are converted to a summary report, which is then printed. (Rajoppi Test., 2/26 Trial Tr. at 42:1-7, 61:20-21.)

619. Ms. Rajoppi also receives the results tapes that are printed from each of Union County's DREs. (Rajoppi Test., 2/26 Trial Tr. at 63:3-5.) The results tapes list individual candidate totals from a given district, and also list the turnout totals for each party, Democrat and Republican. (Rajoppi Test., 2/26 Trial Tr. at 68:10-14.)

620. The party turnout totals appear under the heading "Option Switch Totals" on the results tapes. (Ex. P-54; Rajoppi Test., 2/26 Trial Tr. at 69:12 to 70:4.) Ms. Rajoppi explained at trial how these party turnout totals are recorded. There is a rectangular panel on the Sequoia Advantage containing numbered buttons which are sequenced and activated as necessary for an election. (Rajoppi Test., 2/26 Trial Tr. at 69:13-17.) In a primary election, one of the numbers is designated to be Democratic, and another is designated to be Republican. (Rajoppi Test., 2/26 Trial Tr. at 69:18-21.). Every voter receives a Voting Authority slip which designates them as either a Republican or a Democrat. Based on that authority

slip, the poll worker presses the appropriate button on the DRE to trigger either the Republican or Democratic ballot. (Rajoppi Test., 2/26 Trial Tr. at 70:16-23, 71:14-17.) In both cases, yet another button on the operator panel is subsequently pressed to activate the DRE for the voter. (Id. at 71:18 to 73:4.)

621. In order to verify the results of an election before she certifies them, on the day after an election, Ms. Rajoppi and her staff compare the vote total data contained on the results tapes – including the Option Switch Totals – against the data on the summary reports, to ensure that these numbers correlate. (Rajoppi Test., 2/26 Trial Tr. at 52:13-16, 63:10-14.) Ms. Rajoppi performs this check for every election. (Rajoppi Test., 2/26 Trial Tr. at 66:23-25.)

622. Ms. Rajoppi is not responsible for reading the absentee ballots. These ballots go directly to the Board of Elections, which reads them using optical-scan equipment. (Rajoppi Test., 2/26 Trial Tr. at 53:14-24.) Ms. Rajoppi was responsible for purchasing the optical-scan equipment for Union County in 2003, and has been satisfied with the optical-scan results. (Rajoppi Test., 2/26 Trial Tr. at 54:8-12.)

623. The Board of Elections sends Ms. Rajoppi its vote totals for the absentee ballots in the evening of Election Day. (Rajoppi Test., 2/26 Trial Tr. at 61:20 to 62:1.) Approximately two to four days after that, the provisional ballots are read. (Rajoppi Test., 2/26 Trial Tr. at 62:2-5.)

624. For a general election, Ms. Rajoppi testified that the results must be certified by the Monday following an election. For a primary election, the results must be

certified within ten days after the election. (Rajoppi Test., 2/26 Trial Tr. at 51:16-23.)

D. Ms. Rajoppi's Discovery of the Sequoia Advantage "Option Switch Bug" After the February 2008 Presidential Primary Election, and her Efforts to Have it Investigated

625. After the close of the polls for the Presidential primary election that took place in New Jersey on February 5, 2008, Ms. Rajoppi and her staff went about their routine of validating the results from the cartridge readers by comparing the data contained in the summary reports to that contained in the results tapes. (Rajoppi Test., 2/26 Trial Tr. at 66:17-22.)

626. On this occasion, however, Ms. Rajoppi and her staff found that for at least nine districts within Union County, the results tape data and the summary report data did not correspond completely. (Rajoppi Test., 2/26 Trial Tr. at 66:17-22, 83:5-10.)

627. At trial, Ms. Rajoppi explained the discrepancy by examining the data from the results tape for Cranford, District 27. (Rajoppi Test., 2/26 Trial Tr. at 70; Ex. P-54.)

628. On that results tape, the Option Switch Totals showed that 55 Republicans and 170 Democratic voters had voted in that district. (Rajoppi Test., 2/26 Trial Tr. at 70:1 to 71:9.) However, Ms. Rajoppi pointed out that when the candidate totals from that district are added, the result is 57 votes for Republican candidates and 168 votes for Democratic candidates. (Id. at 73:12 to 74:16.)

629. Ms. Rajoppi also testified that in five of the nine districts experiencing discrepancies between results report and summary report data, there were fewer

voting authority slips than votes on the cartridge – meaning that there were more votes tabulated than there were voters. (Id. at 75:10-15.)

630. As a result of these discrepancies, Ms. Rajoppi was concerned that she could not certify the election results to be true and valId. (Id. at 88:15-18.)

631. Ms. Rajoppi reported the vote total discrepancies in nine districts in Union County to the Attorney General's Office as soon as they were discovered, within one or two days after the election. (Id. at 84:3-12.) Ms. Rajoppi spoke either to Donna Kelly or someone in her office and conveyed that she had discovered a problem that did not appear to be confined to Union County. Ms. Rajoppi requested the assistance of the Attorney General's Office in resolving the problem. (Id. at 84:20 to 85:6.)

632. Ms. Rajoppi contacted the Attorney General's office three to four times over the course of a month, and spoke to different individuals. On one occasion, Ms. Rajoppi spoke to Karen DuMars, and suggested that the Attorney General's Office assume the lead in conducting an investigation to uncover the source of the errors that Ms. Rajoppi had discovered. (Id. at 85:20 to 86:13.) Nonetheless, nobody from the Attorney General's office ever contacted Ms. Rajoppi concerning her suggested investigation. (Id. at 86:14-23.)

633. Immediately upon her discovery of the discrepancies, Ms. Rajoppi also contacted Joe McIntyre, Sequoia's account manager assigned to Union County. (Id. at 83:24-84:2, 87:21-23.) Ms. Rajoppi explained that she needed to know why the errors occurred, because she was concerned about certifying the election. (Rajoppi Test., 2/26 Trial Tr. at 88:11-18.)

634. At trial, when asked whether Sequoia adequately explained to her the cause of the errors she discovered, Ms. Rajoppi responded: "Absolutely not." (Id. at 89:7.) Ms. Rajoppi does not believe that the Attorney General's Office answered her concerns regarding what caused the errors during the February 2008 Presidential primary. (Id. at 89:11-15.)

635. As a result of what she believed to be inadequate explanation and response to the issue on the part of Sequoia and the Attorney General's Office, Ms. Rajoppi was compelled to modify the language normally used in her certification of an election. (Id. at 89:17-20.) Ms. Rajoppi used this modified language in her certification of the February 2008 Presidential primary election results to reflect the discrepancies she had found, because she "could not swear that it was accurate." (Id. at 89:19-23.)

636. Dissatisfied with the response she had received from Sequoia and the Attorney General's Office, Ms. Rajoppi took action herself to obtain answers regarding what caused the errors she had discovered. (Id. at 89:24-90:3.)

637. Ms. Rajoppi spoke with colleagues from what she considered a random sample of counties, both Democrat and Republican, large and small. (Id. at 90:5-8.) She asked her colleagues if they had found discrepancies, and explained to them how she found discrepancies in Union County by correlating the results tapes to the summary reports. (Id. at 90:22 to 91:9.)

638. Ms. Rajoppi also petitioned the Constitutional Officers Association to pass a resolution urging the Attorney General or the Secretary of State to conduct an independent investigation into the errors that occurred with Sequoia Advantage

DREs during the February 2008 Presidential primary. (Id. at 91:19-24.) The Executive Committee of the Constitutional Officers Association took a vote on the proposed resolution, and as a result, the Constitutional Officers Association took a position advocating for an independent investigation. (Id. at 92:11-13.) The Constitutional Officers Association conveyed this position by letter and resolution to the Attorney General's Office and the Secretary of State. (Id. at 92:13-14.) Ms. Rajoppi helped draft the letter. (Id. at 94:18 to 95:4; Ex. P-56.)

639. Ms. Rajoppi testified that she voted for the Constitutional Officers Association's resolution because she believed that an independent investigation by a state agency was necessary for voters to have confidence in their voting machines. (Rajoppi Test., 2/26 Trial Tr. at 96:13-19.)

640. Ms. Rajoppi testified that the State never performed an independent investigation in Union County. (Id. at 96:24 to 97:17.) Consequently, in pursuit of an independent investigation of the Sequoia Advantage DREs, Ms. Rajoppi conducted research to find an appropriate person to perform the investigation. She looked for someone who was an expert on DREs and who had done research on the Sequoia Advantage or similar machines, who had written reports, and who had a scientific background. (Id. at 98:14-22.)

641. Ultimately, Ms. Rajoppi's research led her to contact Professor Edward Felten of Princeton University to determine if this "respected computer scientist" would be interested in conducting such an investigation. (Id. at 97:24.)

642. After his conversation with Ms. Rajoppi, Professor Felten submitted requests under the Open Public Records Act ("OPRA") to Ms. Rajoppi's office, seeking the results tapes from the DREs in question. (Id. at 99:10 to 100:7.)

643. However, certain individuals – including Donna Kelly – attempted to dissuade Ms. Rajoppi from retaining Professor Felten to perform an independent investigation of Sequoia Advantage DREs. (Id. at 100:19-20, 102:3-7.) After consultation with Union County Counsel and counsel for the Constitutional Officers Association, Ms. Rajoppi changed her course of action and did not retain Professor Felten. (Id. at 101:9-13.)

644. Ms. Rajoppi testified that the short-circuiting of her proposed independent investigation has impacted her job as County Clerk: she has to certify elections but questions the reliability and accuracy of the Sequoia Advantage DREs. (Id. at 102:19 to 103:2.)

E. Problems With the Sequoia Advantage DRE Discovered by Ms. Rajoppi During the June 2008 Primary Election n in Union County

645. In the June 2008 primary election in Union County, a candidate named Carlos Cedeño ran for the office of Freeholder. (Id. at 103:10-17, 104:7.) The office of Freeholder is a county-wide position, meaning that Mr. Cedeño name was on every ballot. (Rajoppi Test., 2/26 Trial Tr. at 104:7-11.)

646. However, in the summary reports generated from the ballot cartridges, Mr. Cedeño's name did not appear at all. (Id. at 105:5.) Ms. Rajoppi believes that this error occurred because of the tilde accent appearing in Mr. Cedeño's last name. (Id. at 103:16-20.)

647. As a Count Clerk, Ms. Rajoppi testified that the fact that Mr. Cedeño's name did not appear on the summary report is "quite serious." (Id. at 105:6-8.)

648. Ms. Rajoppi testified that the remedies for this issue suggested by Sequoia were unacceptable to her. (Id. at 107:19-22.) Nonetheless, Sequoia produced a technician on election night to "hand-edit" the results." Ms. Rajoppi and her staff had no knowledge of what "hand-editing" was, but had to open up the tally of the election to a representative of Sequoia. (Id. at 108:5-15.)

649. Even at trial, Ms. Rajoppi could not testify to what the Sequoia technician had actually done with the election results. (Id. at 109:10-14.) Nobody from her office has ever received any information on how to "hand-edit" election results. (Id. at 109:18-19.)

650. Consequently, Ms. Rajoppi does not have 100% confidence in her certification of the Freeholder's election. (Id. at 110:23-25.)

651. Another incident involving the Sequoia Advantage DREs occurred in Union County after the November 2008 general election. (Id. at 111:2-6.)

652. On the day following that election, Ms. Rajoppi's staff discovered that all of the results from all 438 ballot cartridges that had been tabulated the night before were no longer in the WinEDS computer – the results of the election had been reset, or "zeroed out." (Id. at 111:13 to 112:3, 113:15-16, 115:15-18.)

653. Ms. Rajoppi testified that it was not possible that the results were not saved in the first instance. (Id. at 114:7-9.) Summary reports had already been run from the results; "[a]ll of the figures were there, and the next morning they were gone." (Id. at 113:8-11.)

654. Ms. Rajoppi had not authorized anyone in her office to reset the election results. (Id. at 112:9-11.) Moreover, to reset the results would be a "very involved process," with several warning messages appearing on the computer screen asking the user whether she truly wanted to reset the results. (Id. at 114:9-17.)

655. As a result of this incident, Ms. Rajoppi and her staff were compelled to read all 438 ballot cartridges again. (Id. at 117:1-2.)

656. In addition to the loss of vote tallies, Ms. Rajoppi received many complaints regarding the Sequoia Advantage DREs on Election Day during the November 2008 General Election, including several complaints from the Mayor of Springfield alone. (Id. at 117:15 to 120:13.)

657. As a result of the myriad problems that she experienced during three different elections in 2008, Ms. Rajoppi – the official charged with certifying to the accuracy and reliability of election results in Union County – testified that she does not have confidence in the Sequoia AVC Advantage. (Id. at 65:24 to 66:11.)

VIII. Testimony of James Everett Clayton

658. James Everett Clayton is the supervisor of the Ocean County voting machine warehouse. He is not a computer scientist, a computer security expert, or a computer engineer. (Testimony of James Clayton ("Clayton Test."), Feb. 26, 2009 Trial Tr. at 178:9-16, 180:22-25, 182:5-12.)

659. Mr. Clayton was a witness for the Defendants. Plaintiffs' cross-examination was limited to the scope of the Defendants' direct examination.

660. Mr. Clayton is a former politician from Point Pleasant, Ocean County and currently one of two partisan coordinators at the voting machine warehouse in Ocean County. (Clayton Test, 2/26 Trial Tr. at 178:20-23, 182:13 to 183:11.)

661. Mr. Clayton supervises the warehouse where Ocean County's Sequoia AVC Advantage 9.00H DREs are stored. (Clayton Test, 2/26 Trial Tr. at 182:5-12, 183:24 to 184:1.) He is also responsible for ensuring these DREs are properly maintained and prepared for every election. (Id.)

662. Neither he nor his staff has received any formal, independent training on the operations of the Sequoia AVC Advantage DRE or the WinEDS system. (Clayton Test, 2/26 Trial Tr. at 180:9-14, 183:12-17, 183:24 to 184:1, 190:20 to 191:5.)

663. Mr. Clayton does not know how votes are recorded on the Sequoia AVC Advantage DRE. (Testimony of James Clayton ("Clayton Test."), Mar. 3, 2009 Trial Tr. at 55:15-18.)

664. Mr. Clayton is not qualified to assess whether a Sequoia AVC Advantage DRE computer has been corrupted or otherwise tampered with. (Clayton Test, 3/3 Trial Tr. at 84:15 to 85:2.)

665. The acceptance testing which Mr. Clayton and his staff perform on the Sequoia AVC Advantage DREs is nothing more than Sequoia's suggested testing protocol; it is not an independent analysis of the DREs' accuracy or reliability. (Clayton Test, 3/3 Trial Tr. at 84:22 to 85:2.)

666. Mr. Clayton testified that Ocean County's Sequoia AVC Advantage DREs have security measures, such as tamper-evident tape and seals. (Clayton Test, 3/3 Trial Tr. at 95:5-7.) Mr. Clayton claims he has never seen any evidence of seal tampering, but Mr. Clayton is not a security expert. (Clayton Test, 3/3 Trial Tr. at 67:12 to 68:15, 75:9-16, 96:11-14.)

667. Mr. Clayton has never consulted a security expert to examine seals or tape for tampering and he has no formal training on detecting seal tampering. (Clayton Test, 3/3 Trial Tr. at 96:7-14.)

668. During Mr. Clayton's testimony, the State represented to the Court that the security measures (seals, tape, and strap seals) used in Ocean County by Mr. Clayton were considered and abandoned by the State..

669. Mr. Clayton admitted that the Sequoia AVC Advantage DRE can be altered to display inaccurate information. Mr. Clayton admitted that both its protective counter, which is a record of the total number of votes cast through the life of a DRE and its date- and time-setting can be reset. (Clayton Test., 2/26 Trial Tr. at 243:25 to 244:4; Clayton Test., 3/3 Trial Tr. at 97:16-19.)

670. Mr. Clayton testified that every results cartridge in Ocean County has a precinct I.D. code and a number matching the Sequoia AVC Advantage DRE in which it is used. (Clayton Test., 2/26 Trial Tr. at 217:5-18.) The results cartridges are

numbered to prevent a technician from inserting the wrong results cartridge into a DRE. (Clayton Test., 3/3 Trial Tr. at 99:20-23.) Mr. Clayton lacks the expertise to know if the numbering system is a security measure that prevents fraud. (Clayton Test, 3/3 Trial Tr. at 99:13 to 100:1.)

671. Ocean County has been using the same results cartridges for many years. (Clayton Test., 2/26 Trial Tr. at 195:15-17.)

672. Mr. Clayton admitted that the ROM chips can be removed from the Sequoia AVC Advantage DRE motherboard, if someone gains access to the back of the machine. (Clayton Test., 3/3 Trial Tr. at 95:8-17.) Despite this security threat, neither he nor his staff keeps a record of the ROM chip serial numbers or regularly inspects the ROM chips, to see if they have been tampered with or altered. (Clayton Test, 3/3 Trial Tr. at 91:21 to 92:11.) In fact, there is not even a seal covering the ROM chips, from which tampering could be detected. (Clayton Test, 3/3 Trial Tr. at 92:12-14.)

673. The computer server used to create the ballot is located at an Ocean County administrative building, which Mr. Clayton does not oversee. (Clayton Test., 2/26 Trial Tr. at 191:18 to 192:3.)

674. The four laptops and two desktop computers used to prepare the results cartridges with ballot information and to download election results from results cartridges to the Board of Elections after the election can be connected to the Internet. (Clayton Test., 2/26 Trial Tr. at 190:16-19, 192:9-16; Clayton Test., 3/3 Trial Tr. at 87:1-7.) Mr. Clayton has never checked whether his staff uses the Internet on these computers. (Clayton Test, 3/3 Trial Tr. at 89:1-4.)

675. The Pre Logic Accuracy Testing ("Pre-LAT") performed by Mr. Clayton and his staff on the Sequoia AVC Advantage DREs does not ensure that the DREs will accurately tally the votes. (Clayton Test, 3/3 Trial Tr. at 79:20 to 80:9.) Mr. Clayton admitted that he and his staff do not press every button and/or switch located on the DRE to determine if doing so registers a vote for a particular candidate even if that button or switch is not assigned to that particular candidate. (Clayton Test, 3/3 Trial Tr. at 82:22 to 83:8.) Though Mr. Clayton is neither a computer scientist nor computer security expert, he personally trained his technicians how to perform Pre-LAT. (Clayton Test., 2/26 Trial Tr. at 178:9-16, 237:8-11.) He instructed them to select all the candidates in one column and then move sequentially across the ballot; he did not instruct them to vary the manner in which they selected the buttons to push during the Pre-LAT simulated voting because "[i]t would be very easy to become confused if you don't use a standard method of moving across." (Clayton Test, 2/26 Trial Tr. at 233:21 to 234:12.) He employs this Pre-LAT method not because it ensures accuracy, reliability, or safety, but because he believes it is the "simplest way to go across." (Clayton Test, 2/26 Trial Tr. at 237:8-11.)

676. In Ocean County, manual Pre-LAT tests are generally not performed on the Sequoia AVC Advantage DREs. Instead, the County uses simulation cartridges to conduct Pre-LAT testing. (Clayton Test, 2/26 Trial Tr. at 237:12-16, 241:10-17.) The simulation program is generated through Sequoia's WinEDS program. (Clayton Test., 3/3 Trial Tr. at 8:7-25.) Like the manual Pre-LAT procedures, the same simulation script is used for each DRE in the County and the script is

written so the same voting pattern is applied to each DRE. (Clayton Test., 2/26 Trial Tr. at 240:3-6, 240:18-25.)

677. Typically, Mr. Clayton writes the simulation script to cast between eight and fifteen votes per candidate. (Clayton Test., 3/3 Trial Tr. at 83:13-20.) The simulation scripts are written to test only buttons that are recommended by the WinEDS system; it does not test all the buttons on the voting machine. (Clayton Test, 3/3 Trial Tr. at 83:5-8.)

678. Pre-LAT tests performed in Ocean County in preparation for the February 5, 2008 Presidential primary did not uncover the option switch bug, which allowed for a greater number of votes than voters to be recorded by the Sequoia AVC Advantage DREs. (Clayton Test, 3/3 Trial Tr. at 85:10-18.)

679. To prevent the option switch bug from occurring again, a plastic shield was added to the back of the operator panel. (Clayton Test, 3/3 Trial Tr. at 85:19-22.) During a primary, the shield is supposed to prevent a poll worker from pressing a button other than for the parties participating in the primary. (Clayton Test., 2/26 Trial Tr. at 230:3-13.) The shield, however, is attached to the machine by Velcro and is easily removable. (Clayton Test., 3/3 Trial Tr. at 85:23 to 86:2.) Mr. Clayton has not developed a protocol to ensure that the shield remains in place on Election Day. (Clayton Test, 3/3 Trial Tr. at 86:3-9.)

680. The storage procedures that have been instituted by Mr. Clayton for the Sequoia AVC Advantage DREs are specific to Ocean County; they are not universally applied across New Jersey. (Clayton Test, 3/3 Trial Tr. at 78:25 to 79:4.) In addition, many of Ocean County's Sequoia AVC Advantage DRE security

policies and procedures are not memorialized in writing. (Clayton Test, 3/3 Trial Tr. at 78:12-24, 79:5-6.)

681. Mr. Clayton does not have personal knowledge of the voting policies and procedures followed in other New Jersey counties.

682. Ocean County owns 818 Sequoia AVC Advantage DREs of which approximately 767 are used during an election. (Clayton Test., 2/26 Trial Tr. at 184:23-25.)

683. Irrespective of any controls Mr. Clayton has imposed at the Ocean County voting machine warehouse (Clayton Test., 3/3 Trial Tr. at 70:16 to 74:19.), neither Mr. Clayton nor his staff have control over the more than 750 DREs while the DREs are at the polling locations.

684. Given the number of DREs in polling locations in Ocean County, at least one week is needed before each election to distribute all of the DREs. At least one week is needed to collect the DREs after each election. (Clayton Test, 3/3 Trial Tr. at 33:12-16, 36:21-25.)

685. Neither Mr. Clayton nor his staff has control over the security of the Sequoia AVC Advantage DREs during the nearly two weeks that they are at the polling locations. Mr. Clayton acknowledged that "there is no one to watch over" the DREs at polling locations, and he has never seen a surveillance video camera at a polling location, despite the fact that the DREs are, in some instances, left in a public "large, open cafeteria-type room." (Clayton Test, 3/3 Trial Tr. at 78:8-11, 77:2-10, 77:18 to 78:2.)

686. Mr. Clayton admitted he has neither drafted nor is he aware of any written policies for storing or securing DREs at polling locations, and he does not employ

a log book to record the names of those who access each polling site where DREs are delivered. (Clayton Test, 3/3 Trial Tr. at 76:11-14, 76:24 to 77:1.)

687. Mr. Clayton does not know what policies are followed at each voting location in Ocean County. He does not directly train or instruct the Election Day poll workers. (Clayton Test, 3/3 Trial Tr. at 44:17.) Nor has he witnessed the Election Day poll opening procedure at every election precinct. (Clayton Test, 3/3 Trial Tr. at 44:18-25, 45:1-13.)

688. Mr. Clayton has never witnessed the poll-closing procedures. (Clayton Test, 3/3 Trial Tr. at 58:2-6.)

689. Even though Mr. Clayton testified that he and his technicians prepare a poster explaining voting procedures for the AVC Advantage, Mr. Clayton does not know whether (or how) this poster is actually displayed at polling locations in Ocean County. (Clayton Test, 3/3 Trial Tr. at 49:2-18.)

690. Similarly, Mr. Clayton does not know if the sample ballot displayed at a voting location includes voting instructions or whether it identifies the grid positions in which the candidates' names appear. (Clayton Test, 3/3 Trial Tr. at 55:7-14.)

IX. Testimony of Robert Francis Giles

691. Robert Francis Giles is the Director of the New Jersey Division of Elections, a position under the authority of the Secretary of State's Office. (Testimony of Robert Francis Giles ("Giles Test."), March 3, 2009 Trial Tr. at 110:23-24, 117:15-16.)

692. Mr. Giles testified for Defendants. Plaintiffs' cross-examination of Mr. Giles was limited to the very few subjects raised on direct examination.

A. Background and Experience

693. Mr. Giles received a Bachelor of Arts in Psychology from Denison University. He has not received any post-graduate degrees or certifications in any subject matter. (Giles Test., 3/3 Trial Tr. at 111:16.)

694. Despite the fact that every county in New Jersey uses DREs and DREs are computer-based systems, Mr. Giles does not possess any degrees or certifications in computer science or computer engineering. (Giles Test., 3/3 Trial Tr. at 111:19, 137:24 to 138:4.) Mr. Giles does not know how to fix computers or their circuitry. (Giles Test., 3/3 Trial Tr. at 138:5-17.) Mr. Giles does not know how to program a computer in any computer language. (Giles Test., 3/3 Trial Tr. at 138:5-7.) Mr. Giles has not written a computer program since 1986, when he wrote a simple program for a college class. (Giles Test., 3/3 Trial Tr. at 137:24 to 138:4.)

695. Mr. Giles does not have any background in computer security. (Giles Test., 3/3 Trial Tr. at 137:17-23.)

696. After graduating from college, Mr. Giles spent the first eight years of his career working construction jobs. (Giles Test., 3/3 Trial Tr. at 111:23 to 112:5.)

697. In 1995, he took a job at the Ocean County Board of Elections as an investigator. (Giles Test., 3/3 Trial Tr. at 112:8-15.) As an investigator, Mr. Giles tracked down individuals whose ballots were returned as undeliverable. (Giles Test., 3/3 Trial Tr. at 112:18-24.) He performed these duties for eight months before becoming a voting machine technician. (Giles Test., 3/3 Trial Tr. at 112:25 to 113:1.)

698. As a voting machine technician for Ocean County, Mr. Giles worked with the county's optical scan machines to set up the machines prior to an election, conduct Pre-LAT tests, perform whatever maintenance was required, and deliver the optical scan machines to polling places. (Giles Test., 3/3 Trial Tr. at 113:6-10.)

699. Mr. Giles worked as a voting machine technician for only eight months, until he was offered the position of assistant supervisor to the Ocean County Board of Elections. (Giles Test., 3/3 Trial Tr. at 114:1-4.)

700. As assistant supervisor to the Ocean County Board of Elections, Mr. Giles worked as an administrator. (Giles Test., 3/3 Trial Tr. at 114:7-10.) Mr. Giles was promoted to supervisor of the Board of Elections, in 1999, despite having no educational background or formal training in computers or DREs. (Giles Test., 3/3 Trial Tr. at 116:22-25, 111:17-19.)

701. In May 2008, Mr. Giles was appointed to his current job as Director of the New Jersey Division of Elections. (Giles Test., 3/3 Trial Tr. at 116:6-25.)

B. Responsibilities as Director of Division of Elections Include Certifying DREs for Use in the State

702. In his position as Director of the New Jersey Division of Elections, Mr. Giles is responsible for, among other things, coordinating the certification process for DRE vendors who want to certify DREs in the State. (Giles Test., 3/3 Trial Tr. at 121:25 to 122:11.) When contacted by a vendor requesting certification, Mr. Giles schedules a hearing before the Title 19 Committee. (Giles Test., 3/3 Trial Tr. at 122:2-11.) He orders a transcriber and arranges a meeting place. (Id.) Mr. Giles passes certification materials from the vendors to the Title 19 Committee. (Id.)

703. Members of the Title 19 Committee are appointed by the Secretary of State. (Giles Test., 3/3 Trial Tr. at 124:19-20.)

704. The Title 19 Committee bases its entire technical knowledge of DREs on materials presented by the vendors, including ITA reports. (Giles Test., 3/3 Trial Tr. at 159:1-8.) The Title 19 Committee does not conduct its own examination of the software in any DRE. (Giles Test., 3/3 Trial Tr. at 159:1-8.) The State of New Jersey does not conduct independent testing of DREs prior to their certification to determine whether the DREs are "hackable." (Giles Test., 3/3 Trial Tr. at 159:25 to 160:3.)

705. Sequoia DREs are computer-based systems. (Giles Test., 3/3 Trial Tr. at 139:1.) However, owing to his extremely limited experience and education relating to computers and electronics, Mr. Giles does not understand all of the technical material contained in ITA reports. (Giles Test., 3/3 Trial Tr. at 159:9-13.)

706. Mr. Giles is unsure whether hackability is tested by the ITAs. (Giles Test., 3/3 Trial Tr. at 159:23-24.)

707. Mr. Giles is aware of, but has not read, the reports issued by the States of California and Ohio criticizing certain DREs certified by New Jersey. (Giles Test., 3/3 Trial Tr. at 144:4-11.)

708. Mr. Giles has never conducted research on DREs that have been decertified by other states. (Giles Test., 3/3 Trial Tr. at 145:14-15.)

709. Neither Mr. Giles nor any member of the Secretary of State's Office conducts any research regarding whether Sequoia DREs have been decertified and decommissioned by other States. (Giles Test., 3/3 Trial Tr. at 145:5 to 146:9.)

710. If an upgrade or improvement is made to a DRE used in New Jersey, Mr. Giles believes that the vendor must seek recertification from the Title 19 Committee. (Giles Test., 3/3 Trial Tr. at 146:24 to 147:6.) However, unless a vendor approaches the State to ask for recertification of its DRE, no such recertification hearing is scheduled. (Giles Test., 3/3 Trial Tr. at 148:5-8.) The Secretary of State's Office relies, therefore, on vendors' self-reporting of software upgrades before any DRE is re-examined by the Title 19 Committee. (See Id.)

711. Mr. Giles is unaware of when and how frequently the Sequoia DREs used by New Jersey have been updated. (Giles Test., 3/3 Trial Tr. at 148:21-23.)

712. Furthermore, Mr. Giles does not know whether the current Sequoia DREs need to be recertified. (Giles Test., 3/3 Trial Tr. at 147:22-24.)

C. No Uniform State Procedures Exist for the Storage, Set-up, and Transportation of DREs

713. There is no uniform statewide policy regarding storage procedures for DREs in county warehouses. (Giles Test., 3/3 Trial Tr. at 152:21-24.)

714. There is no uniform statewide policy regarding the storage of keys that operate the DREs. (Giles Test., 3/3 Trial Tr. at 153:4-7.)

715. There is no uniform statewide policy regarding the transportation of DREs to and from polling locations. (Giles Test., 3/3 Trial Tr. at 153:8-12.) Transportation procedures vary from county to county. (Giles Test., 3/3 Trial Tr. at 153:13-16.)

716. Counties hire private moving companies to transport the Sequoia DREs to and from polling locations. (Giles Test., 3/3 Trial Tr. at 155:24 to 156:4.) There is no statewide requirement that security checks be performed on the employees of the private moving companies. (Giles Test., 3/3 Trial Tr. at 156:5-8.)

717. The State does not mandate a uniform procedure for conducting Pre-LAT tests. (Giles Test., 3/3 Trial Tr. at 154:3-11.) The Division of Elections has not issued any directives as to how many votes should be cast in a Pre-LAT test. (Giles Test., 3/3 Trial Tr. at 158:1-4.)

718. Although there is a statewide board worker training manual, it only addresses poll worker functions, such as what time to arrive on election morning. It does not contain specifics about the DREs. (Giles Test., 3/3 Trial Tr. at 155:3-17.) Additionally, no one from the Division of Elections investigates poll worker compliance with the training manual. (Giles Test., 3/3 Trial Tr. at 155:20-23.)

719. There is no uniform statewide policy for the storage of results cartridges that are used in the AVC Advantage DREs. (Giles Test., 3/3 Trial Tr. at 157:1-8.)

720. There is no uniform statewide policy for the transportation of results cartridges from polling sites to the various county clerks' offices. (Giles Test., 3/3 Trial Tr. at 157:10-13.)

721. Throughout the State of New Jersey, results cartridges are used to determine the vote totals at the end of each election. (Giles Test., 3/3 Trial Tr. at 161:6-9.)

722. The Division of Elections has not issued any directives with regard to connecting the computers and laptops used by counties for transmitting and receiving sensitive election data to the Internet. (Giles Test., 3/3 Trial Tr. at 157:17-25.)

723. There is no statewide procedure for conducting recounts. (Giles Test., 3/3 Trial Tr. at 162:8-10.)

D. Security for the State's 11,000 DREs

724. Mr. Giles is responsible for researching and selecting security measures for the Sequoia DREs, despite the fact that he has no experience with computer security. (Giles Test., 3/3 Trial Tr. at 125:8-17, 137:17-23.)

725. As late as "late summer" of 2008, before the November Presidential election, no statewide, uniform security plan existed in New Jersey. (Giles Test., 3/3 Trial Tr. at 127:1-3, 128:11.) Each county was responsible for choosing if, and how, they implemented their own security procedures. (Giles Test., 3/3 Trial Tr. at 126:16-17, 126:23-24.)

726. In an attempt to standardize security procedures, Mr. Giles "kind of" spoke with counties to see what procedures they had been using. (Giles Test., 3/3 Trial Tr. at 127:2-7.) Mr. Giles's interaction was not with representatives from each of New Jersey's twenty-one counties but rather with five or six members of the New

Jersey Association of Election Officials Voting Machine Committee. (Giles Test., 3/3 Trial Tr. at 127:10-12, 162:16 to 163:9.)

727. After consultation with a single vendor, Brooks, but without any participation by any computer security experts, Mr. Giles settled upon the following security measures:

- Large cup seals;
- Tamper-evident tape; and
- Metal multi-lock cable seals.

(Giles Test., 3/3 Trial Tr. at 130:10-12; 163:10 to 164:4; 164:13-15.)

728. The State abandoned these security measures shortly after adopting them. (Giles Test., 3/3 Trial Tr. at 131:25 to 132:5; 165:23 to 166:4.)

729. The tamper-evident tape recommended by Brooks and purchased by the State for the November 2008 election was chosen because of its success in securing airplanes overnight. (Giles Test., 3/3 Trial Tr. at 166:13-23.) Subsequently, however, the adhesive proved to be too weak to secure the Sequoia DREs. (Giles Test., 3/3 Trial Tr. at 166:13-23.)

730. Mr. Giles is "experimenting" with different types of tamper-evident tape. (Giles Test., 3/3 Trial Tr. at 132:7-9.) Mr. Giles has asked the vendor to combine features of different tape seals, but nothing has been finalized. (Giles Test., 3/3 Trial Tr. at 132:15-16.) The State would like to use tape that is both strong and recognizable, but no such tape is currently in production. (Giles Test., 3/3 Trial Tr. at 132:6-16.)

731. For upcoming elections, Mr. Giles is considering the following security measures, again, without any consultation or participation by any computer security expert:

- Small cup seals (1/2 inch);
- Brooks blue padlock, which Mr. Giles refers to as a "high security padlock"; and
- Tamper-evident tape.

(Giles Test., 3/3 Trial Tr. at 132:2-5.)

732. None of these seals are currently in use on DREs in the State of New Jersey. (Giles Test., 3/3 Trial Tr. at 133:12 to 135:16, 174:6-19.) Despite the fact that Mr. Giles has read Dr. Johnson's report regarding serious security issues with the padlocks, the State is moving forward on procuring the padlocks from Brooks. (Giles Test., 3/3 Trial Tr. at 176:3-7.)

733. Although Mr. Giles claims that the small cup seal exists and can be imprinted with three digits at an additional cost to the State, (Giles Test., 3/3 Trial Tr. at 134:19, 165:14-20), Mr. Giles has never seen a small cup seal with any serial numbers. (Testimony of Robert Giles ("Giles Test.") May 11, 2009 Trial Tr. at 74:2.)

734. Mr. Giles has not placed an order for the small cup seals. (Giles Test., 5/11 Trial Tr. at 73:18-20.)

735. Mr. Giles has not put the cup seals out to bid. (Giles Test., 5/11 Trial Tr. at 73:21-22.)

736. Mr. Giles has not consulted with any independent security expert to formulate an inspection procedure for any seals and locks contemplated for use in New Jersey. (Giles Test., 3/3 Trial Tr. at 170:1-6.) At present, no inspection procedures exist for examining seals or locks intended for use on the DREs. (Giles Test., 3/3 Trial Tr. at 169:16-25.)

E. Funds Are Available That Could Be Used to Purchase Auditable DREs

737. Since 2002, New Jersey has received between $80-$90 million in federal funds under the Help American Vote Act to upgrade its voting systems and election administration. (Giles Test., 3/3 Trial Tr. at 139:9-13.)

738. Approximately $19 million of these funds remain available for use by New Jersey. (Giles Test., 3/3 Trial Tr. at 139:6-16.)

739. Mr. Giles testified that the HAVA funds could be used "to replace New Jersey's voting machines with a different kind of system that is more accurate and reliable." (Giles Test., 3/3 Trial Tr. 139:14 to 140:3.)

X. Testimony of Richard C. Woodbridge

740. Richard Woodbridge is an appointed member of the Title 19 Voting Machine Certification Committee ("Title 19 Committee" or the "Committee"). He was first appointed to the Title 19 Committee in 1982. (Testimony of Richard C. Woodbridge ("Woodbridge Test."), March 4, 2009 Trial Tr. at 6:7-16.)

741. Mr. Woodbridge testified on behalf of Defendants. Plaintiffs' cross-examination of Mr. Woodbridge was limited to the very few subjects raised on direct examination.

742. TheTitle 19 Committee evaluates voting machines to ensure that they comply with the mandates of N.J.S.A. §§ 19:48-1 and 19:53A-3. (Woodbridge Test., 3/4 Trial Tr. at 19:12-25.)

743. For each voting machine that it evaluates, the Title 19 Committee generally prepares a report indicating whether, in its opinion, the voting machine meets the statutory requirements of Title 19. (Woodbridge Test., 3/4 Trial Tr. at 11:7-11.) If a DRE has been previously examined by the Committee, the Committee does not always conduct a full certification hearing for the machine when changes are made. (Woodbridge Test., 3/4 Trial Tr. at 80:16 to 83:23.)

744. Mr. Woodbridge has served as the chairperson of the Title 19 Committee for the past ten or twelve years and he drafts the Committee's reports. The other Committee members sign off on Mr. Woodbridge's reports. (Woodbridge Test., 3/4 Trial Tr. at 9:13-25.)

745. Mr. Woodbridge did not apply to be a member of the Title 19 Committee. The Secretary of State appointed him to serve on the Committee in 1982. (Woodbridge Test., 3/4 Trial Tr. at 30:3-4.)

746. Mr. Woodbridge has never been provided with formal feedback or a review of his performance as a member of the Title 19 Committee. (Woodbridge Test., 3/4 Trial Tr. at 31:8-15.)

747. The State of New Jersey has never run a conflicts check on Mr. Woodbridge related to his service as a member of the Title 19 Committee. (Woodbridge Test., 3/4 Trial Tr. at 32:2-4.)

748. Mr. Woodbridge declined to recuse himself from Title 19 Committee proceedings involving A-1 Technology, despite the fact that he had previously represented the company for approximately two years in his private practice as a patent attorney on non-voting machine matters. (Woodbridge Test., 3/4 Trial Tr. at 32:8 to 33:3.)

749. Mr. Woodbridge has never been provided with formal training relating to his duties as a member of the Title 19 Committee. (Woodbridge Test., 3/4 Trial Tr. at 33:14-24.)

750. Mr. Woodbridge is a patent attorney. (Woodbridge Test., 3/4 Trial Tr. at 7:6-13.)

751. Mr. Woodbridge is not a computer security expert. (Woodbridge Test., 3/4 Trial Tr. at 29:10-19.)

752. Mr. Woodbridge is not a computer scientist. (Woodbridge Test., 3/4 Trial Tr. at 29:20-23.)

753. Mr. Woodbridge has never written any computer programming source code. (Woodbridge Test., 3/4 Trial Tr. at 28:9-15.)

754. The makeup of the Title 19 Committee varies depending on who is available to participate. (Woodbridge Test., 3/4 Trial Tr. at 31:4-7.) Since 1982,

approximately twelve or fifteen other individuals have served on the Title 19 Committee with Mr. Woodbridge. (Woodbridge Test., 3/4 Trial Tr. at 8:11-14.)

755. Mr. Woodbridge reads all materials that are provided to him in advance of the Title 19 Committee's meetings, but he does not understand everything he reads. (Woodbridge Test., 3/4 Trial Tr. at 17:8-11.)

756. The Title 19 Committee does not consult with computer scientists before making a recommendation to the Attorney General or the Secretary of State as to whether or not a particular DRE should be certified. (Woodbridge Test., 3/4 Trial Tr. at 41:19 to 42:10.)

757. The Title 19 Committee does not examine the software or the source code of DREs before it makes a recommendation to the Attorney General or the Secretary of State as to whether or not the machines should be certified. (Woodbridge Test., 3/4 Trial Tr. at 42:21 to 43:5.)

758. Mr. Woodbridge is unsure of the scope of testing performed on DREs by Wyle Laboratories, an independent testing authority ("ITA"). Specifically, he is uncertain as to whether Wyle examines the DREs' software. (Woodbridge Test., 3/4 Trial Tr. at 43:12 to 44:11.)

759. For a time, Ciber served as New Jersey's independent test authority ("ITA") for the software in DREs. (Woodbridge Test., 3/4 Trial Tr. at 44:12 to 45:9.)

760. Ciber has been decertified as an ITA. (Woodbridge Test., 3/4 Trial Tr. at 44:22-24.)

761. After Ciber was decertified, the Title 19 Committee did not take any action to determine the accuracy of the Ciber reports that it previously relied upon in

making recommendations as to whether certain voting machines should be certified. (Woodbridge Test., 3/4 Trial Tr. at 44:25 to 45:9.)

762. The Title 19 Committee has never conducted any independent research to determine whether DREs used in New Jersey have been unsuccessfully used in other states. (Woodbridge Test., 3/4 Trial Tr. at 45:17-23.)

763. The Title 19 Committee does not have a procedure for independently determining whether voting machines were declined for certification by other states. (Woodbridge Test., 3/4 Trial Tr. at 46:8-25.)

764. Mr. Woodbridge does not recall ever reading reports that were issued by the States of California or Ohio concerning security issues related to the ES&S iVotronic or the Sequoia Edge DREs. (Woodbridge Test., 3/4 Trial Tr. at 52:3-13.)

765. The Title 19 Committee does not perform periodic examinations of voting machines after they have been certified unless the vendor requests a review. (Woodbridge Test., 3/4 Trial Tr. at 56:9-13.)

766. When a vendor requests a review of a machine that has been previously recommended for certification by the Committee, the Committee has the ability to review the earlier reports it issued about that particular voting machine. (Woodbridge Test., 3/4 Trial Tr. at 68:5 to 69:9.)

767. Mr. Woodbridge could not recall if he always read the Committee's previous reports before deciding on whether to recommend voting machines for re-certification. (Id.)

768. Mr. Woodbridge could not recall having examined a previous report prepared by the Title 19 Committee for the Sequoia AVC Advantage DRE when it was presented to the Committee for a recommendation on re-certification in 1987. (Woodbridge Test., 3/4 Trial Tr. at 72:15 to 73:22.)

769. The Title 19 Committee's 1987 report on the Sequoia AVC Advantage DRE states that "[a] similar machine was alleged to have been previously approved by the Secretary of State." (Ex. P-57 at 2.)

770. The Title 19 Committee's evaluation of the Sequoia AVC Advantage DRE in 1987 lasted only two hours. (Woodbridge Test., 3/4 Trial Tr. at 74:7 to 75:2; Ex. P-57 at 1.)

771. The Title 19 Committee did not consult with any computer scientist or computer security experts during the course of its 1987 evaluation of the AVC Advantage. (Woodbridge Test., 3/4 Trial Tr. at 75:6-18; see generally Ex. P-57.)

772. The Title 19 Committee convened on March 2, 2005 to evaluate changes in the tabulation system used to tabulate votes cast on the Sequoia AVC Edge and Advantage DREs and to determine whether it should make a recommendation regarding certification without a full certification hearing. (Woodbridge Test., 3/4 Trial Tr. at 80:16 to 84:1.)

773. After meeting for a mere 45 minutes on March 2, 2005, the Title 19 Committee determined that it could proceed without a full certification hearing. (Woodbridge Test., 3/4 Trial Tr. at 83:24 to 84:11.)

774. Neither Mr. Woodbridge nor any other member of the Title 19 Committee reviewed the revised software or source code during its evaluation of the

tabulation system on March 2, 2005 prior to recommending that it be certified for use in the State of New Jersey. (Woodbridge Test., 3/4 Trial Tr. at 84:17 to 85:5.)

775. The Title 19 Committee did not consult with any computer scientist or computer security experts concerning the revised software or source code for the tabulation system in March 2005 prior to recommending that it be certified for use in the State of New Jersey. (Woodbridge Test., 3/4 Trial Tr. at 84:12-16.) Mr. Woodbridge described this decision as a "no-brainer." (Woodbridge Test., 3/4 Trial Tr. at 84:15-16.)

776. The Title 19 Committee did not examine ITA reports concerning the revised software or source code during its evaluation of the tabulation system in March 2005 prior to recommending that it be certified for use in the State of New Jersey. (Woodbridge Test., 3/4 Trial Tr. at 85:6-10.)

777. Mr. Woodbridge knows that John Fleming, another member of the Title 19 Committee, who is employed by the New Jersey Attorney General's Office, has some technical background but he is unsure of the extent of his technical education or work history. (Woodbridge Test., 3/4 Trial Tr. at 92:10 to 93:13.)

XI. Sequoia Employees Edwin Smith and Paul Terwilliger

A. The State's Eleventh Hour Adoption of Sequoia Employees as its Expert Witnesses

778. Until the commencement of the trial, the State never indicated any intent to call Edwin Smith and Paul Terwilliger (collectively, the "Sequoia Witnesses") as expert witnesses in support of its case.

779. On January 27, 2009, just before the start of trial, the Court ruled that the State's identified expert, Dr. Michael Shamos, would not be allowed "to testify as to whether in his opinion the voting machines are scientifically accurate or reliable." (Colloquy Jan. 27 Trial Tr. at 38:4-6.)

780. A week later, on February 4, 2009 at 6:04 p.m., four days into trial, and after being in Court with Plaintiffs' counsel all day, Plaintiffs' Counsel received (via email) a letter from Ms. Gore stating that the "State defendants intend to call Sequoia representatives Ed Smith and Paul Terwilliger as experts in our case-in-chief." This was the very first time that Plaintiffs were notified in writing of the State's intention to convert Mr. Smith and Mr. Terwilliger from fact witnesses into expert witnesses. Plaintiffs raised the issue with the Court first thing in the morning on February 5, 2009. (Colloquy Feb. 5, 2009 Trial Tr. at 4:13-6:3.)

B. The Sequoia Witnesses' Are Biased

1. Edwin Smith's Personal Stake in the Outcome of this Litigation

781. Mr. Smith is a member of Sequoia's senior management team; he has been Sequoia's vice-president of Compliance since May 2006. (Smith Test., 3/18 Trial Tr. at 16:11-17, 54:17-19.)

782. In addition to the salary that he receives from Sequoia, Smith has received bonuses from Sequoia. Smith's bonus is based on Sequoia's revenue and profit in a given year. (Smith Test., 3/18 Trial Tr. at 54:22 to 55:6.)

783. Moreover, Mr. Smith has an ownership interest in Sequoia. (Smith Test., 3/18 Trial Tr. at 54:14-16.)

784. According to Mr. Smith, Sequoia has sold approximately 10,400 DREs to counties within the State of New Jersey. (Smith Test., 3/18 Trial Tr. at 55:13-16.) Although the New Jersey market accounts for a somewhat variable percentage of Sequoia's annual sales depending upon sales made in other parts of the country, Smith admitted that the New Jersey market accounted for roughly 20 percent of Sequoia's gross annual sales in 2008. (Smith Test., 3/18 Trial Tr. at 58:6 to 59:15)

785. As such, Mr. Smith, held out as an expert witness on behalf of the State, has admitted that he has a personal stake in the outcome of this litigation. The outcome of this case will affect Sequoia's gross annual sales. He benefits from Sequoia's sales in two ways: As an owner of the company, and also in the amount of his bonus. (Smith Test., 3/18 Trial Tr. at 56:24 to 57:3, 59:16-20.)

786. The Court acknowledged Mr. Smith's interest in the outcome of this litigation, and indicated that Mr. Smith's testimony must be weighed accordingly. (Smith Test., 3/18 Trial Tr. at 82:11-15.)

787. As an employee of Sequoia, Mr. Smith could not express agreement even with the most immutable of Professor Appel's conclusions regarding Sequoia DREs. For example:

a. Even Mr. Terwilliger agreed with Professor Appel's assessment that negative vote totals can manipulate elections. (Testimony of Paul Terwilliger ("Terwilliger Test."), March 30, 2009 Trial Tr. at 166:16-19.) Mr. Smith, on the other hand, claimed to disagree with that assessment. (Smith Test., March 19, 2009 Trial Tr. at 138:23-25 to 139:4.)

b. Mr. Terwilliger also agreed with Professor Appel's assessment that problems with the Advantage's daughterboard need immediate attention. (Terwilliger Test., 3/30 Trial Tr. at 166:8-11.) Mr. Smith, on the other hand, would not agree with Professor Appel's assessment. (Smith Test., 3/19 Trial Tr. at 138:15-17.) Yet at the same time, Mr. Smith admitted that he is not familiar with flash memory on the daughterboard; he only "read somewhere that it is present." (Smith Test., 3/19 Trial Tr. at 140:2-11.) Mr. Smith testified, and expressed disagreement with Dr. Appel, on a matter in which he admits he has no expertise (or even familiarity), challenging basic computer science principles.

2. Edwin Smith's Inconsistent Testimony

788. Because of the State's rebranding of Messrs. Smith and Terwilliger as its experts after the trial had already started, the Court permitted the Plaintiffs to re-depose these two witnesses so as to eliminate the element of surprise from the trial. (See colloquy 1/24 Trial Tr. at 10:12-20.)

789. Mr. Smith provided inconsistent and sometimes irreconcilable answers to questions posed at both his deposition and trial. A few examples are listed below:

c. At his deposition, Mr. Smith testified that New Jersey accounts for approximately 20 percent of Sequoia's gross annual sales. But when asked about this at trial, Mr. Smith said "I believe it's around 10 percent." When confronted with this inconsistency, Mr. Smith revised his answer. He admitted that that in 2008, the number was probably around 20 percent, adding the qualification that the number could fluctuate annually depending upon sales in other parts of the country. (Smith Test., 3/18 Trial Tr. at 58:6 to 59:15.)

d. Mr. Smith testified at trial that he is familiar with the 1990 federal voting machine standards. (Smith Test., 3/18 Trial Tr. at 171:17-20.) However, at his deposition, Mr. Smith testified: "I'm not entirely familiar with the 1990 standards as they predate me to some degree." (Smith Test., 3/18 Trial Tr. at 172:2-6.) Smith attempted to explain this inconsistency by asserting that since his deposition, he had become familiar with the 1990 standards. (Smith Test., 3/18 Trial Tr. at 172:11-15.)

e. At trial, Mr. Smith claimed that he was able to explain precisely how the Advantage misgenerated party turnout totals during the February 2008 primary election in New Jersey. (Smith Test., 3/18 Trial Tr. at 172:13-18.) In fact, he claimed that he actually examined that issue himself personally from the moment it was discovered. (Smith Test., 3/18 Trial Tr. at 127:20 to 130:22.) At his deposition, however, when asked to explain whether Democratic votes reported in the Republican primary because of the so-called "option switch bug," Mr. Smith answered: "I don't have enough detail familiarity with how the software misgenerated the party turnout totals to answer your question." (Smith Test., 3/18 Trial Tr. at 174:1-3.) Mr. Smith also stated during his deposition: "I am not familiar with that level of detail, though I do understand Union County had some issues with their party turnout totals." (Smith Test., 3/18 Trial Tr. at 175:2-4.) Mr. Smith did not explain how he went from only a vague understanding that Union County "had some issues" at his deposition, to testifying at trial that he personally dealt with these issues when they were discovered, and to speaking at length about the precise nature and cause of those issues.

f. When asked at trial whether a field programmable gate array chip ("FPGA") could function in the same manner as a Z80 if it is placed into an Advantage DRE, Mr. Smith initially responded: "I do not believe so if it is placed in an Advantage." (Smith Test., 3/18 Trial Tr. at 199:3-4.) But at his deposition, when confronted with the very same question, Smith had answered: "I haven't seen that reduced to practice but in theory, yes." (Smith Test., 3/18 Trial Tr. at 199:10-14.) When confronted with this discrepancy at trial, Mr. Smith admitted that an FPGA could, "in theory," mimic a Z80 when placed in an Advantage. (Smith Test., 3/18 Trial Tr. at 199:16-17.)

g. When asked at his deposition whether fraudulent firmware can be designed so as to avoid detection, Mr. Smith answered in the affirmative. (Smith Test., 3/18 Trial Tr. at 193:10-14.) Yet at trial, Mr. Smith suggested that this would be perhaps "theoretically possible" but "extremely, extremely difficult." (Smith Test., 3/18 Trial Tr. at 193:6-7.) When confronted with the fact that he had revised his testimony, Mr. Smith answered that he felt the Court deserved a fuller explanation than that which he had provided at his deposition (Smith Test., 3/18 Trial Tr. at 193:12-14), notwithstanding Mr. Smith's obligation to provide full and accurate answers to the questions posed to him at his deposition.

C. Mr. Terwilliger's Bias as Reflected by Prior Unlawful Acts Performed on Behalf of Sequoia

790. Dating from the time that Mr. Terwilliger worked at Sunrise Laboratories – approximately 18 years ago – all or substantially all of Mr. Terwilliger's income

has derived from his work performed on behalf of Sequoia. (Terwilliger Test., 3/30 Trial Tr. at 67:24 to 68:14.)

791. From 1997 to 2007, when Mr. Terwilliger was an employee of Sequoia, his bonuses were at least in part a function of the company's sales performance. (Terwilliger Test., 3/30 Trial Tr. at 68:20-22.)

792. Mr. Terwilliger currently serves as a consultant for Sequoia, and is currently working on a firmware modification for the Sequoia Advantage D10. (Terwilliger Test., 3/30 Trial Tr. at 69:17-18.)

793. Mr. Terwilliger presently has no source of income other than the compensation that he receives from Beattie Padovano, Sequoia's counsel in this lawsuit, for his service as an advisor/expert witness in this litigation, and the pay that he receives from Sequoia for his consulting services. (Terwilliger Test., 3/30 Trial Tr. at 69:19 to 70:5.)

794. Although Mr. Terwilliger was held out as an expert witness for the State, he was not compensated by the State for his services – he was compensated by Sequoia's lawyers. (Terwilliger Test., 3/30 Trial Tr. at 70:6-20.)

795. Sequoia's lawyers paid Mr. Terwilliger $150 per hour for his services in this litigation, including his trial testimony. (Ex. P-70 at Schedule A.)

796. Moreover, Mr. Terwilliger admitted that although he is purportedly testifying on behalf of the State, he takes his direction from Arthur Chagaris (Sequoia's counsel), Ed Smith, and Michelle Shaffer – Sequoia's Director of Communications. (Terwilliger Test., 3/30 Trial Tr. at 72:20 to 73:3.)

797. In 2003, during the course of his employment with Sequoia, Mr. Terwilliger personally registered to himself the following Internet domain names: dieboldelection.com, dieboldelections.com, dieboldvote.com, and dieboldvotes.com. (Terwilliger Test., 3/30 Trial Tr. at 74:15-18.)

798. Mr. Terwilliger admits that all of the aforementioned domain names are simply variations on "Diebold," which is one of Sequoia's primary competitors. (Terwilliger Test., 3/30 Trial Tr. at 74:19-24.)

799. Mr. Terwilliger admits that his actions constituted "cyber-squatting." (Terwilliger Test., 3/30 Trial Tr. at 73:17-22.) Cyber-squatting is illegal pursuant to the Anti-Cyber-Squatting Consumer Protection Act of 1999, codified at 15 U.S.C. § 1125(d.)

800. Diebold filed a legal proceeding against Terwilliger before the World Intellectual Property Organization ("WIPO"). (Terwilliger Test., 3/30 Trial Tr. at 75:5-8.)

801. The WIPO panel ruled that the domain names must be turned over to Diebold, finding that Mr. Terwilliger had registered the names in *bad faith*. (Terwilliger Test., 3/30 Trial Tr. at 75:9-77:9.)

802. Although Mr. Terwilliger registered these domain names personally, he testified that he registered them at the direction of Sequoia officials. (Terwilliger Test., 3/30 Trial Tr. at 74:4-12.) As noted at ¶796, supra, Mr. Terwilliger admits that he takes his direction from Sequoia officials in terms of his involvement in this litigation.

D. Sequoia's October 2, 2008 Submission

1. Sequoia's October 2, 2008 Submission Bears no Indicia of an Expert Report, but Rather, is Akin to a Marketing Piece

803. On October 2, 2008, Sequoia filed a document (the "Sequoia Response") with the Court, the "purpose" of which was to "provide a response to the Plaintiff's [sic] report in a lawsuit against the State of New Jersey regarding voting equipment." (Ex. D-17, at 1.)

804. Sequoia had not been invited by the Court to submit any kind of Expert Report or response to Professor Appel's Expert Report, nor did it ever seek permission to do so. The State also never requested that Sequoia be permitted to file an Expert Report. And the State did not submit the Sequoia Response as its own Expert Report.

805. The Sequoia Response does not identify itself as an Expert Report, nor was Sequoia told by the State of New Jersey that it was drafting an Expert Report. (Smith Test., 3/19 Trial Tr. at 34:21 to 35:10.)

806. Unlike the Shamos Report and Professor Appel's Report, the Sequoia Response does not contain any background or qualifications of the authors or any information about the compensation received for services in generating the report. Indeed, the Sequoia Response is unsigned and devoid of authorship.

807. Mr. Smith testified that he received no compensation for preparing the Sequoia Response other than his regular salary – paid for by Sequoia. (Smith Test., 3/19 Trial Tr. at 36:6-11) The Sequoia Response was plainly drafted in Mr. Smith's normal course of employment, not in any capacity as an expert witness at trial.

808. Nowhere does the Sequoia Response state that it is being submitted on behalf of the State of New Jersey. To the contrary, it is quite clear that the document is issued on behalf of Sequoia itself – even the heading is the same banner attached to Sequoia's press releases.

809. Although Sequoia's counsel represented in a letter dated October 2, 2008 that the Sequoia Response had been authored by Mr. Smith and Mr. Terwilliger only, both of the Sequoia Witnesses admitted at trial that the document had a third author – Michelle Shaffer, Sequoia's Director of Communications and an owner of the company. (Terwilliger Test., 3/30 Trial Tr. at 78:13-14; Smith Test., 3/18 Trial Tr. at 83:13-15.)

810. Mr. Terwilliger admitted that Michelle Shaffer was not only an author of the Sequoia Response, but that she made the "final edits" to that document. (Terwilliger Test., 3/30 Trial Tr. at 78:13-18, 91:6 to 92:12.) Mr. Terwilliger could not, or would not, pinpoint precisely which sections she drafted. (Terwilliger Test., 3/30 Trial Tr. at 91:6-92:12.) Mr. Smith, on the other hand, would admit only that Ms. Shaffer only "assisted with editing." (Smith Test., 3/18 at 83:13-15.)

811. Mr. Terwilliger admitted that other unidentified Sequoia employees were also responsible for some of the representations made in the Sequoia Response. (Terwilliger Test., 3/30 Trial Tr. at 157:20-24.)

2. The Ambiguous Authorship of the Sequoia Response Resulted in a Lack of Accountability for its Representations, Particularly the Inflammatory Language Used Therein

812. The lack of authorship and accountability in the Sequoia Response caused the Plaintiffs to spend a great portion of their cross-examinations of Mr. Smith and

Mr. Terwilliger trying to ascertain precisely which portion of the Sequoia Response each witness drafted. Messrs. Smith and Terwilliger had particular difficulty standing behind some of the most vociferously asserted – indeed inflammatory – portions of the Sequoia Response.

813. The document refers derogatorily to Professor Appel and his team as "the academics" (as though their affiliation with Princeton University somehow discredits them), but Mr. Terwilliger appeared to blame that term on the absent Michelle Shaffer. (Terwilliger Test., 3/30 Trial Tr. at 83:7.)

814. Mr. Terwilliger claimed to have authored Section 11.11 of the Sequoia Response. But when confronted with some particularly inflammatory language from that section, which referred to Professor Appel's findings as "egregiously intellectually dishonest," Terwilliger disclaimed responsibility for that particular language, and claimed that he could only guess as to who was responsible. (Terwilliger Test., 3/30 Trial Tr. at 91:3-14.)

815. As to Section 11 of the Sequoia Response (a section which accuses Professor Appel of being "misleading" and of holding back critical facts), Mr. Terwilliger stated that although he contributed to it, most of the words were not his. He was unsure who authored the inflammatory words. (Terwilliger Test., 3/30 Trial Tr. at 89:14-18.)

816. Like Mr. Terwilliger, Mr. Smith also disclaimed responsibility for the use of inflammatory and offensive language in the Sequoia Response. Although Mr. Smith admitted that he "may have" drafted content at Section 5.7 (a section which accuses Dr. Appel of a "lack of rigor") of the Sequoia Response related to the

plastic strap seal, Mr. Smith could not, or would not, say whether it was he or someone else who actually drafted that section. (Smith Test., 3/19 Trial Tr. at 14:2-15.)

817. Mr. Smith also disclaimed responsibility for the use of the word "farcical" in the Sequoia Response to refer to Professor Appel's work, but could not identify who had written that word. (Smith Test., 3/18 Trial Tr. at 21:18 to 22:4.)

3. No Opinions Are Rendered in the Sequoia Response. The Response Consists of Inflammatory Conclusions that the Sequoia Witnesses Could Not Defend at Trial

818. Mr. Smith admitted that he performed no tests of any kind in connection with the assertions made in the Sequoia Response. (Smith Test., 3/19 Trial Tr. at 39:6-17.)

819. Concomitant with the lack of any testing, Mr. Smith also testified that there is no data in the Sequoia response save for the sound level of tones emitted from the Advantage. (Smith Test., 3/19 Trial Tr. at 42:4-25 to 43:1-3.)

820. Mr. Terwilliger further testified that he performed no measurements, experiments or tests in connection with the Sequoia Response (save for instructing someone to measure the sound level of the Advantage's speaker). (Terwilliger Test., 3/30 Trial Tr. at 114:12-18.)

821. The Sequoia Response rests largely on the accusation that Professor Appel's findings are moot because the security protections were removed from the machines prior to his study. (Ex. D-17 at 2, 4.) The Sequoia Response reaches the bold conclusion that Professor Appel's experiments and findings concerning the ease with which he could replace legitimate firmware with fraudulent firmware on the Advantage are "null and void" because, allegedly, a factory-

installed security screw and seal were removed from the machine tested by Professor Appel. (Ex. D-17 at 4; Smith Test., 3/19 Trial Tr. at 10:20 to 11:2.)

822. When questioned about these strong words at trial, Mr. Terwilliger admitted that he had "no reason to believe that [Professor Appel] removed any security seals that might have been present before he did his demonstrations." (Terwilliger Test., 3/30 Trial Tr. at 87:12-14.)

823. Indeed, the Court's very own Order made clear that the State was to turn over to Professor Appel two DREs in the same state they were in for the February 5, 2008 Presidential Primary election.

824. Additionally, when confronted with the fact that Professor Appel had demonstrated in the courtroom that he could get through those very security devices, Mr. Smith (who had allegedly authored the pertinent section of the Sequoia Response), admitted that he was not present to see Dr. Appel defeat these security measures, but that he had heard from Mr. Terwilliger that this had occurred. (Smith Test., 3/19 Trial Tr. at 10:20 to 11:10.)

825. Further, the Sequoia Response attacks Professor Appel's claims that his students were able to reverse engineer 20 percent of the Advantage's code. (Ex. D-17 at 8.) At trial, Mr. Terwilliger testified that he did not request Professor Appel's work product in order to determine the legitimacy of this claim, nor did he provide any basis for doubting it.

826. The Sequoia Response, at Section 12.14, asserts that "Sequoia's surveillance likewise has not detected any fake processor chips that would be suitable to cause an AVC Advantage to malfunction." (Smith Test., 3/19 Trial Tr. at 24:17-20.) At

trial, Mr. Smith admitted that his definition of "surveillance" is unique – it simply refers to the fact that Mr. Smith reviews "literature," which he more fully described as a series of security and technology-related emails that he receives. Mr. Smith, also admitted that even under his definition of the word, none of this so-called "surveillance" was performed in New Jersey. (Smith Test., 3/19 Trial Tr. at 24:23 to 25:4.)

827. Although the Sequoia Response discusses the use of widely available election validation software that can be employed to protect the integrity of the vote, Mr. Terwilliger testified that such software is used in Nevada on the Sequoia *Edge*, and that he is unaware of similar software being used with the Advantage. (Terwilliger Test., 3/30 Trial Tr. at 97:20 to 98:17.)

828. The Sequoia Response also curtly dismisses Professor Appel's discussion of fraudulent Z80 processor chips as "fantasy" in a matter of three sentences. (Ex. D-17 at 9.) The lack of basis for this out-of-hand rejection is apparent when viewed in light of the fact that, several months subsequent to the filing of the Sequoia Response, Mr. Terwilliger authored a second Expert Report, the majority of which is devoted to addressing the threat of fraudulent processor chips. (D-23; See ¶¶ 829-839, infra.)

E. Paul Terwilliger's February 19, 2009 Expert Report

1. Everything in the Terwilliger Report Could Have Been Raised Earlier, in the Sequoia Response, Rather Than in the Middle of a Trial

829. On or about March 10, 2009, in response to Plaintiffs' discovery request that corresponded with the Court permitting Messrs. Smith and Terwilliger to testify as experts on February 23, 2009, Sequoia's attorneys (not the State) emailed to

the Plaintiffs an "Expert Report" drafted by Mr. Terwilliger (the "Terwilliger Report"). The Terwilliger Report is dated February 19, 2009 – after Mr. Terwilliger had the benefit of watching Professor Appel testify for several days.[21]

830. The Terwilliger Report was purportedly submitted on behalf of the State of New Jersey, notwithstanding the fact that it was drafted under the supervision of Sequoia's attorney, Arthur Chagaris. (Terwilliger Test., 3/30 Trial Tr. at 140:1-2.)

831. Mr. Terwilliger admitted that everything he addressed in the Terwilliger Report could have been raised in the Sequoia Response in October 2002. Initially, Mr. Terwilliger gave some excuses for not addressing these points earlier, in the Sequoia Response. (Terwilliger Test., 3/30 Trial Tr. at 141:2 to 143:9.) Ultimately, however, when pressed on why he failed to respond to these sections of Professor Appel's Report in the Sequoia Response, Terwilliger responded: "I don't have a good answer for that." (Terwilliger Test., 3/30 Trial Tr. at 143:10-12.)

2. The Terwilliger Report's Proposed Methods of Detecting Fraudulent Z80s – Also Reflected in Smith's PowerPoint Presentation – are Highly Suspect

832. As described by Mr. Smith, a "Z80" is the microprocessor within the Advantage Version 9 that "interprets the firmware, the voter's input, [and] the inputs of the poll worker through the operator panel and executes whatever the firmware says."

---

[21] Plaintiffs have never received any explanation as to why Sequoia's attorneys allowed 15 days to pass after the Court's February 23rd ruling before supplying Plaintiffs with this Expert Report, particularly where the report was signed and dated February 19, 2009, and where the Court had expressed abundant concern with allowing Plaintiffs a fair opportunity to respond to new expert opinions unveiled in the middle of a trial.

(Smith Test., 3/18 Trial Tr. at 147:4-7.) Professor Appel's Report describes a method by which an FPGA can be made to act as a counterfeit Z80, which could be used to manipulate the vote.

833. Notwithstanding his preparation of a detailed PowerPoint presentation designed to demonstrate purported methods for detecting fraudulent Z80s, at trial, Smith would not retract or alter his original assertion that the entire notion of a fraudulent Z80 created from an FPGA is "all a fantasy" and "science fiction." (Smith Test., 3/19 Trial Tr. at 46:1, 74:14-16.)

834. Mr. Terwilliger, on the other hand, now admits: "I agree with Plaintiffs' Expert Report that an FPGA can be made to act like a Z80. This [program] appears to be freely available as the "T80" project at www.opencores.org." (D-23 at 6.)

835. Both the Terwilliger Report and a PowerPoint presentation prepared by Mr. Smith identify a number of ways in which a fraudulent Z80 purportedly could be detected. To wit:

a. Delidding: With this method, nitric acid is dripped onto the center of a chip in order to dissolve its cover; the "heart" of the chip is then examined to determine its authenticity. (Ex. D-23 at 7-8; Smith Test., 3/18 Trial Tr. at 147:25.) Mr. Smith testified that one could look with the naked eye at the etchings on the chip to determine its authenticity, or look at the chip under a microscope. (Smith Test., 3/18 Trial Tr. at 148:14-17.)

b. X-ray: With this method, a chip – or the entire circuit board that the chip is installed on – is examined with an x-ray machine to determine its authenticity. (D-23 at 9-10.) Mr. Smith testified that with this method, one could compare the wafer size of two chips, the wires that join the "wafer" of the chip to the "legs" which protrude from it, as well as the legs themselves. (Smith Test., 3/18 Trial Tr. at 150:15-21.)

c. ROM Replacement: With this method, Mr. Terwilliger speculates that one could discover a fraudulent Z80 by replacing the ROM chip that ordinarily handles powering up the Advantage with one that immediately does something visible, like turning on a light. (D-23 at 11.) Presumably, Mr. Terwilliger believes that the fraudulent Z80 would expose itself by

executing the normal power-up process, rather than following the instruction of the new ROM.

d. Electromagnetic Radiation: With this method, the Sequoia witnesses propose that a fraudulent Z80 would likely radiate a different pattern (frequencies, amplitudes) than a genuine Z80, and could thus be exposed with equipment designed to ascertain the pattern of the voting machine's electromagnetic radiation. (D-23 at 11; Smith Test., 3/18 Trial Tr. at 163:10-13.)

836. Mr. Smith testified:

> It is my opinion that if you had a suspect machine and you thought that the Z80 had been de-soldered, removed, replaced by a fraudulent chip and re-soldered back in, you could indeed…take just that suspect Z80 chip to a laboratory that either does delidding or x-ray or both…

(Smith Test., 3/18 Trial Tr. at 153:2-9.) However, Mr. Smith did not testify as to how one would know in the first instance that the chip is "suspect." To the contrary – the Sequoia Witnesses both testified that an ordinary observer would not be able to ascertain that a Z80 chip might have been replaced with a fraud. Specifically, Mr. Smith testified that the asserted difference in dimension between a Z80 and an FPGA could not be ascertained by the naked eye. (Smith Test., 3/19 Trial Tr. at 55:2-7.) Mr. Terwilliger also admits that an "FPGA could be repackaged to mimic the Z80's packaging so that to an untrained observer they look identical." (Terwilliger Report, at 10; see also Smith Test., 3/19 Trial Tr. at 57:12-21.)

837. Mr. Smith had not considered how many DREs New Jersey would need to test, using any of the methods identified, in order to be reasonably certain that no fraud had been committed. (Smith Test., 3/18 Trial Tr. at 202:10 to 204:22; Smith Test., 3/19 Trial Tr. at 47:2-6.)

838. Mr. Terwilliger testified that he did not conduct any studies to determine, nor did he consider at all, whether any of these methods would be either practical or cost effective to implement. (Terwilliger Test., 3/30 Trial Tr. at 135-36.)

839. The Sequoia Witnesses also identified numerous other weaknesses in their proposed Z80 detection methods (in addition to the fundamental problems

identified by Plaintiffs' expert Professor Wolf, whose testimony is summarized at ¶¶ 1212-1256, supra.) To wit:

a. Delidding:

- To Mr. Smith's knowledge, no state has ever used delidding to test their voting machines for fraudulent firmware. (Smith Test., 3/19 Trial Tr. at 44:20-23.)
- Mr. Smith admitted that delidding is a destructive testing process; a chip is no longer useful once this test has been performed. (Smith Test., 3/18 Trial Tr. at 200:20 to 201:3.)
- Mr. Smith testified that delidding would require the removal of the chip or the entire circuit board from the DRE, and that the chip or the circuit board would then have to be sent off-site for testing. (Smith Test., 3/19 Trial Tr. at 48:17-20.)
- Mr. Smith does not know whether any New Jersey voting machine mechanics possess the requisite skill to desolder a Z80 for the delidding process. (Smith Test., 3/19 Trial Tr. at 45:1-8.)
- Although Mr. Smith believed that, if done in bulk, delidding might cost "single dollars per unit," he did not consider in this rough calculation any of the significant labor costs, shipping costs, and administrative expenses associated with this method. (Smith Test., 3/19 Trial Tr. at 48:1-16.)
- Mr. Smith made clear that Sequoia will not offer the service of delidding to its New Jersey customers. (Smith Test., 3/19 Trial Tr. at 44:7-10.) Thus, the State of New Jersey would need to pay a third-party vendor for this service.

b. X-Ray:

- Mr. Smith's PowerPoint slides addressing Z80 chips purport emphasize the difference in appearance between the Z80 chips and FPGAs appearing in those slides. (See Ex. D-19.) However, Mr. Smith admitted at trial that the FPGA "wafer" could be repackaged in a housing that would make it appear like a Z80. (Smith Test., 3/19 Trial Tr. at 57:12-18.) The comparison made by Mr. Smith's PowerPoint presentation, then, is between a Z80 and a much longer FPGA, and not between a Z80 and an FPGA that has been altered to look like a Z80. Both Professors

Wolf and Appel testified that it is simple to make an FPGA look like a real Z80 chip.

- Mr. Smith acknowledged that to use an x-ray to detect a fraudulent Z80, the entire circuit board would need to be removed and sent to an outside entity for testing. (Smith Test., 3/19 Trial Tr. at 48:21-25.)
- Nonetheless, Mr. Smith also speculated (but ultimately did not know) that an x-ray machine could be brought to a voting machine warehouse – despite the fact that these machines are the size of a telephone booth and cost around $300,000. (Smith Test., 3/19 Trial Tr. at 58:14-59:8.)
- Mr. Smith does not know whether there are entities in New Jersey with the capacity to perform x-ray testing for fraudulent Z80s. (Smith Test., 3/19 Trial Tr. at 49:1-3.)
- Mr. Terwilliger testified that he is unaware who manufactures such x-ray machines, and that he has never even *seen* one of these machines. (Terwilliger Test., 3/30 Trial Tr. at 145:1-2.)
- Indeed, Mr. Terwilliger admitted that he held himself out to be an expert on the proposed x-Ray technique, but admitted that in fact, he is not an expert in this area. (Terwilliger Test., 3/30 Trial Tr. at 145:9-18.)

c. Electromagnetic Radiation:

- Mr. Smith admitted that he has never used electromagnetic radiation testing for the purposes of detecting a fake Z80. (Smith Test., 3/19 Trial Tr. at 73:22-25.)
- Mr. Smith admitted that he has never used electromagnetic radiation testing in a forensic sense. (Smith Test., 3/18 Trial Tr. at 166:10.)
- Mr. Smith claimed very generally that he had performed an electromagnetic radiation test on a DRE, yet he proffered no evidence or reports to support this bald assertion. (Smith Test., 3/18 Trial Tr. at 166:18 to 167:22.)
- According to Mr. Smith, no state has ever conducted an electromagnetic radiation test to detect a fake Z80. (Smith Test., 3/19 Trial Tr. at 74:1-3.)
- Mr. Smith admitted that the vast majority of the electromagnetic radiation from the Advantage comes from the wires connecting the chips and the motherboard – not from internal silicon chips ("wafers") themselves. (Smith Test., 3/19 Trial Tr. at 75:9-14.)

- Mr. Terwilliger admitted that he has no knowledge of the radiation levels of an FPGA chip, and thus cannot be sure if this method would be effective in detecting such a chip disguised as a Z80 processor chip. (Terwilliger Test., 3/30 Trial Tr. at 149:15-22.)

F. The Sequoia Witnesses Agree With Professor Appel's Assertion That Software Independence is Critical to Securing New Jersey's DREs

840. Mr. Smith testified that "software independence" is vital to secure voting machines in New Jersey. (Smith Test., 3/19 Trial Tr. at 30:8-11.) Mr. Smith defines "software independence" as:

> [T]he concept that through use of...a second record of the cast votes, that you could count your election and be assured that your tabulation of the election was accurate even if there were known or unknown software bugs, malicious changes to the software, or even inadvertent changes made to the software..., that essentially your ability to recount and check the election is now independent of the software running on the voting machines. (Smith Test., 3/19 Trial Tr. at 29:18 to 30:7.)

841. Mr. Smith opines that a VVPAT is a software independent mechanism. (Smith Test., 3/19 Trial Tr. at 31:3-5.) However, Mr. Terwilliger testified that unlike optical scan voting, where the voter marks the ballot directly, Sequoia's audit trail is dependent on software. (Terwilliger Test., 3/30 Trial Tr. at 84:18 to 86:8.)

G. The Sequoia Witnesses Agree With Professor Appel's Assertion That Hacking Poses a Legitimate Threat to DREs in New Jersey

842. Mr. Smith admitted that hacking poses a real threat to voting machine security in New Jersey. (Smith Test., 3/19 Trial Tr. at 4:14-16.)

843. Mr. Smith testified that during his time working for Hart Intercivic, another DRE manufacturer, the company faced a number of technically skilled hacker attacks daily. (Smith Test., 3/19 Trial Tr. at 6:1-6.)

844. To Mr. Smith's knowledge, none of the hackers who have in the past attacked DRE vendors have been caught. (Smith Test., 3/19 Trial Tr. at 8:1-4.)

845. Mr. Terwilliger agrees that there are several ways in which New Jersey's voting machines can be hacked. (Terwilliger Test., 3/30 Trial Tr. at 159:1-4.)

846. Mr. Terwilliger also agrees with Dr. Appel's assertion that the AVC Advantage can be tampered with in less than seven minutes. (Terwilliger Test., 3/30 Trial Tr. at 162:1-6.)

847. Mr. Terwilliger also testified that he agrees with Dr. Appel's assertion that fraudulent firmware could be present on a machine but may not be detected during a Pre-LAT test. (Terwilliger Test., 3/30 Trial Tr. at 167:21-24.)

H. The Sequoia Witnesses Agree With Professor Appel's Assertion That Many Substantial Changes Have Been Made to the Sequoia Advantage Since it was First Introduced in New Jersey in 1987

848. The Sequoia Advantage was certified in New Jersey in 1987. (Smith Test., 3/18 Trial Tr. at 62:7-10.)

849. Mr. Smith testified that since 1987, the only re-certification in New Jersey that he is aware of occurred in January 2009, when the D10 was certified.[22] (Smith Test., 3/18 Trial Tr. at 62:15-23, 183:23-25.)

850. Mr. Smith also testified that the software in the Advantage has changed since 1987. (Smith Test., 3/18 Trial Tr. at 184:1-3.) Indeed, between 1991 and 1997 alone, Sequoia released too many versions of the Advantage software for Mr. Terwilliger to recall, although he testified that there were "a lot," and more than

[22] As the Court is aware, Plaintiffs' motion seeking a declaratory judgment that the Sequoia Advantage D10 has not in fact been certified by the State of New Jersey is currently pending before the Court.

ten. (Terwilliger Test., 3/30 Trial Tr. at 27:17-28:14.) According to Mr. Smith, these software changes are vital, because software "defines" the behavior of the Advantage, and the DRE could not function without it. (Smith Test., 3/19 Trial Tr. at 191:19-23.)

851. Mr. Smith could not explain why many changes, including bug fixes, to the Advantage software were made after the DRE was certified in 1987. (Smith Test., 3/18 Trial Tr. at 189:21 to 191:15.) As such, Mr. Smith could not confirm whether or not these changes would have required specific approval for implementation in New Jersey under N.J. Stat. 19:53A-4. (Smith Test., 3/18 Trial Tr. at 189:1 to 191:18.)

852. Mr. Smith testified that there are three versions of federal voting systems standards in existence: The Federal Election Commission's 1990 and 2002 standards, as well as the Federal Election Assistance Commission's 2005 standards. (Smith Test., 3/18 Trial Tr. at 90:22 to 91:9.)

853. The Sequoia AVC Advantage 9.00H used in New Jersey was certified only under the 1990 standards. (Terwilliger Test, 3/30 Trial Tr. at 21:8-17.)

854. Mr. Smith admitted that the 2002 standards contain a number of new and enhanced requirements in comparison to the 1990 standards, including, "a number of requirements around software, how software is architected," and "how the hardware is architected, what it has to do." (Smith Test., 3/18 Trial Tr. at 92:21 to 93:3.)

855. Mr. Smith stated that the concept of "reliability" is "standard policy" in the 2002 federal standards. He did not say the same about the 1990 standards. (Smith Test., 3/18 Trial Tr. at 99:16-18.)

856. Mr. Terwilliger testified that the firmware in Version 9.00H of the Advantage could not meet the 2002 federal standards. (Terwilliger Test., 3/30 Trial Tr. at 106:2-3.)

857. Mr. Smith's testimony also identified one particular way in which Sequoia's failure to obtain renewed federal certification of the Advantage 9.00H after myriad software changes/additions could impair the integrity of the DREs used in New Jersey. To wit:

d. Mr. Smith testified about a method of detecting fraudulent ROM chips described as the "hashing method," whereby certain code embedded in software is run through an algorithm which results in a value that is essentially unique to that software, and thus, any manipulation of the software would manifest in the form of a different value. (Smith Test., 3/18 Trial Tr. at 144:13 to 145:8.)

e. Mr. Smith also testified that to perform this check, jurisdictions can obtain the hash values regarding a particular piece of software or firmware "from the federal labs because they're required by the government to hash *all the software that they approved.*" (Smith Test., 3/18 Trial Tr. at 145:9-15) (emphasis added.)

f. However, Sequoia has made numerous changes and additions to the 9.00H DRE's firmware since its approval by a federal lab. Thus, according to Mr. Smith's testimony, the State of New Jersey would not be able to obtain reliable and/or complete hash values from the federal labs for new or updated software components of the Advantage 9.00H, to the extent that those components were not examined and approved as part of the federal certification process.

I. Sequoia's Patchwork Approach to Updating the Advantage Makes the DRE Increasingly Vulnerable

858. Mr. Terwilliger testified that in order to modify New Jersey's Sequoia Advantage 9.00H DREs to make them into a D10, the audio subsystem ("daughterboard") of

the DRE needs to be modified to become the main intelligence of the system, and the original CPU board ("motherboard") then just handles some user interface components. (Terwilliger Test., 3/30 Trial Tr. at 107:24 to 108:7.) Thus, according to Mr. Terwilliger, the motherboard, which usually runs a DRE (or any computer, for that matter), essentially becomes an appendage. (Terwilliger Test., 3/30 Trial Tr. at 113:2-5.)

859. This unorthodox modification is necessary because the Advantage's CPU board is old technology and is resource-starved, lacking the memory to perform necessary functions. (Terwilliger Test., 3/30 Trial Tr. at 127:25 to 128:7.)

860. Converting the daughterboard into the main CPU, however, increases the DRE's dependence on flash memory. According to Mr. Terwilliger, flash memory is highly vulnerable to being changed or overwritten. (Terwilliger Test., 3/30 Trial Tr. at 109:17-18.)

861. Mr. Terwilliger admits that if he were to design a system from scratch, he would not design it to be the D10 and would not make the daughterboard the central processing unit. (Terwilliger Test., 3/30 Trial Tr. at 113:6-8.)

862. Mr. Smith testified that the vote-stealing viruses described in Section 21.8 of Professor Appel's Report would be of limited effect, because they would only affect the blind voters who vote on the audio kit of the Advantage Version 9, which runs on flash memory. (Smith Test., 3/19 Trial Tr. at 31:18 to 32:7.) Increased reliance on flash memory in the D10 – for all votes, not just those of blind voters – most certainly makes the threat of viruses even more real.

863. The Advantage 9.00H also incorporates software from third-party vendors that is not individually tested by Sequoia. Mr. Smith does not know which vendors provide that software; although he "believes" that in addition to Microsoft and Datalight, one of the vendors has "the word 'general' in their name." (Smith Test., 3/18 Trial Tr. at 179:5-13.)

J. The Sequoia Witnesses Agree with Professor Appel's Determination that WinEDS is Vulnerable Because it Can be Connected to the Internet

864. According to Mr. Smith, WinEDS is a software product that is generically known as an election management system. (Smith Test., 3/18 Trial Tr. at 106:9-12.)

865. Among other functions, WinEDS is used to prepare the ballot cartridges which transport the vote totals from the polling place to election headquarters, and to load votes onto the PC. (Smith Test., 3/19 Trial Tr. at 85:13-23.)

866. Mr. Smith testified that running the WinEDS program on computers connected to the Internet constitutes a significant security threat should *never* be run on a computer that is connected to the Internet. (Smith Test., 3/18 at 32:19-22.)

867. Nonetheless, it is possible to connect a computer running WinEDS to the Internet; nothing in WinEDS disables the computer's ability to connect to the Internet. (Smith Test., 3/19 Trial Tr. at 84:13-85:3.)

868. WinEDS does not have built into it any antivirus capability. (Smith Test., 3/19 Trial Tr. at 105:16-18.)

K. Sequoia Has Failed to Adequately Address the "Option Switch Bug"

869. Mr. Smith admitted that the "option switch bug" was a "real problem." (Smith Test., 3/18 Trial Tr. at 129:9.)

870. The Sequoia Witnesses testified that this problem has been addressed in the Advantage D10 firmware. (Smith Test., 3/18 Trial Tr. at 186:16-19; Terwilliger Test., 3/30 Trial Tr. at 125:16-23.)

871. But Sequoia only implemented this change on the Advantage D10 – not the Version 9.00 H DREs machines used in New Jersey. (Smith Test., 3/18 Trial Tr. at 186:12-19.) Mr. Terwilliger testified that Sequoia has taken no steps, relative to Version 9, to correct the firmware problem that caused the option switch error during the February 2008 Presidential primary election in New Jersey. (Terwilliger Test., 3/30 Trial Tr. at 125:5-9.)

872. Mr. Smith testified that Sequoia's solution to the option switch bug problem as to the Version 9 DREs used in New Jersey was to offer the counties a plastic cover that can be placed over the operator to prevent the errant pressing of buttons; however, this plastic cover is removable, attached only by Velcro. (Smith Test., 3/18 Trial Tr. at 129:8 to 130:22.)

873. Mr. Smith testified that the main effect of the option switch bug was that the Advantage was activated with the wrong primary election ballot for many voters. (Smith Test., 3/19 Trial Tr. at 77:16-20.)

874. Mr. Smith also testified that he does not consider the problems caused by the "option switch bug" to be an issue of reliability; rather, he testified that a DRE is "reliable" if "it fires up every time you try to turn it on and it runs." (Smith Test., 3/18 Trial Tr. at 186:16-24.)

875. Mr. Smith gave inconsistent testimony on whether he considers the "option switch bug" to have caused an "inaccuracy." Mr. Smith at first stated that "when the

operator panel is misused by the poll worker and errant buttons are pressed, it does provide an *inaccurate* total." (Smith Test., 3/18 Trial Tr. at 187:12-14.) (emphasis added) Later, he testified that he did not recall ever using the term "inaccurate," and instead testified that although the misreporting of party turnout totals is an "undesirable situation," it does not constitute an inaccuracy. (Smith Test., 3/18 Trial Tr. at 187:22 to 188:3.)

L. Sequoia Withholds Information About Bugs and Vulnerabilities from its New Jersey Customers

876. As testified to by Ms. Joanne Rajoppi, Union County Clerk, candidate Carlos Cedeño's name did not appear on the Summary Report printed in Union County during the June 2008 election. (Rajoppi Test., 2/26 Trial Tr. 103:10-22.)

877. Mr. Smith testified that candidate Cedeño's name was left off of the report because WinEDS randomly assigned him the candidate number "999." (Smith Test., 3/18 Trial Tr. at 133:13 to 134:1.) Mr. Smith admitted that there is no way to know whether a candidate will be assigned that number, and that there is a bug in WinEDS such that a candidate who has been assigned "999" will not appear on the summary report. (Id.)

878. Sequoia knew about this "bug" before it affected Union County. (Smith Test., 3/19 Trial Tr. at 79:19-21.) Notwithstanding Sequoia's awareness of this bug, Sequoia did not issue a product bulletin to its New Jersey customers warning them of this issue until *after* the Carlos Cedeño incident. (Smith Test., 3/18 Trial Tr. at 134:22.)

879. Indeed, Mr. Smith admitted that Sequoia has been aware of many potential weaknesses in its machines that it does not share with its New Jersey customers. To wit:

a. Mr. Smith admitted that although Sequoia has been aware that fraudulent firmware can be installed on the Advantage voting machine, Sequoia has never notified any New Jersey state or county officials of this problem. (Smith Test., 3/18 Trial Tr. at 192:3-11.)

b. Mr. Smith admitted that although Sequoia has been aware that fraudulent firmware can be designed so that it will misallocate only a small number of votes so as to avoid detection, Sequoia has never notified any New Jersey state or county officials of this problem. (Smith Test., 3/18 Trial Tr. at 192:24 to 194:6.)

c. Mr. Smith admitted that although Sequoia has been aware that fraudulent firmware can be designed so that it will escape detection by the Pre-LAT tests performed in New Jersey, Sequoia has never notified any New Jersey state or county officials of this problem. (Smith Test., 3/18 Trial Tr. at 194:7 to 195:2.)

M. The Software Security Measures Identified by the Sequoia Witnesses are Not Inherent in Sequoia's Products, Not Used in New Jersey, Incredibly Time Consuming, and Technically Difficult to Implement[23]

880. Mr. Smith identified a method of protecting the WinEDS system which he referred to as "hardening." He testified that this method would involve making numerous changes to Windows. (Smith Test., 3/18 Trial Tr. at 112:18 to 113:10.)

881. However, these "hardening" procedures, according to Mr. Smith, are only performed in California and Nevada on the Sequoia Edge – not in New Jersey. (Smith Test., 3/18 Trial Tr. at 117:12-13.) Smith does not believe that anyone

[23] Mr. Smith's testimony concerning these protective "hardening" techniques was rebutted by Professor Appel. Professor Appel's rebuttal testimony appears in Section XXX of this document.

from Sequoia has checked to see if New Jersey's counties are implementing any hardening procedures. (Smith Test., 3/19 Trial Tr. at 103:11-14.)

882. Mr. Smith also testified that wiping out and reinstalling Windows and/or WinEDS on the "election central computer" at some point within the election cycle would be another means of guarding against malicious programs. (Smith Test., 3/18 Trial Tr. at 122:5-17.)

883. However, as noted by Mr. Smith, this method is employed in California and Colorado. (Smith Test., 3/18 Trial Tr. at 122:5-10.) Smith has no knowledge of this occurring in New Jersey. (Smith Test., 3/19 Trial Tr. at 117:18-20.)

884. Mr. Smith also pointed to anti-virus software as a means of securing the WinEDS system. (Smith Test., 3/18 Trial Tr. at 118:20 to 119:13.)

885. Notwithstanding Mr. Smith's opinion that antivirus programs are important for the integrity of the DRE, Sequoia does not offer its customers antivirus software as part of its DREs. (Smith Test., 3/19 Trial Tr. at 105:16 to 106:14.)

886. Mr. Smith additionally suggested a safeguard referred to as "firmware validation," whereby a statistical sample of ROM chips is examined at various points during the election cycle to determine whether they have been adulterated in any manner. (Smith Test., 3/18 Trial Tr. at 139:13-22.)

887. But again, Mr. Smith testified that firmware validation is performed, to his knowledge, only in California, Nevada, and Cook County, Illinois. (Smith Test., 3/18 Trial Tr. at 141:21-23, 142:17-20.) Later in his testimony, Mr. Smith corrected his testimony and stated that he was only sure about Nevada. (Smith Test., 3/19 Trial Tr. at 119:4-9.)

888. Mr. Smith admitted that in order to perform firmware validation, one would have to: (1) remove all of the security seals affixed to the circuit board covering the ROM chips – including screws, locks, glue and tape; (2) remove and reinstall the ROM chips; and (3) Install fresh copies of all of the security seals. (Smith Test., 3/19 Trial Tr. at 121:1-11.)

889. Both Professor Appel and Dr. Shamos agree that removing ROM chips from DREs to test them make the ROM chips vulnerable to attack.

N. The State's New Physical Security Measures Might Impair the DRE

890. Mr. Smith admits that he is not familiar with New Jersey's most recent physical security configuration for its DREs. (Smith Test., 3/19 Trial Tr. at 20:1-3.)

891. However, Sequoia has never glued screws into its DREs. (Smith Test., 3/19 Trial Tr. at 64:19-21.)

892. Mr. Smith testified that the State never consulted with Sequoia about applying glue to Sequoia DREs, and what affect that might have on the overall performance of the DREs. (Smith Test., 3/19 Trial Tr. at 65:1-7.)

893. Mr. Smith believes that there is a possibility that the application of glue to the machines could cause problems, depending on how it is applied. (Smith Test., 3/19 Trial Tr. at 64:22-25.)

O. The Sequoia Advantage D10 Has Not Been Certified to 2005 Federal Standards

894. Mr. Terwilliger testified that the D10 alone has been certified under the 2002 federal standards, but did not testify that the D10 with VVPAT has been similarly certified. (Terwilliger Test., 3/30 Trial Tr. at 102:1-13.)

895. Mr. Terwilliger could not explain why Sequoia has not sought to certify the Advantage D10 to the 2005 federal standards. (Terwilliger Test., 3/30 Trial Tr. at 102:14-19.)

896. Mr. Smith testified that "software independence" is vital to secure voting machines in New Jersey. (Smith Test., 3/19 Trial Tr. at 30:8-11.) Mr. Smith defines "software independence" as

> [T]he concept that through use of...a second record of the cast votes, that you could count your election and be assured that your tabulation of the election was accurate even if there were known or unknown software bugs, malicious changes to the software, or even inadvertent changes made to the software..., that essentially your ability to recount and check the election is now independent of the software running on the voting machines.

(Smith Test., 3/19 Trial Tr. at 29:18 to 30:7.)

897. Mr. Smith opines that a VVPAT is a software independent mechanism. (Smith Test., 3/19 Trial Tr. at 31:3-5.) However, Mr. Terwilliger testified that unlike optical scan voting, where the voter marks the ballot directly, Sequoia's audit trail *is* dependent on software. (Terwilliger Test., 3/30 Trial Tr. at 84:18 to 86:8.)

XII. Testimony of Defendants' Expert Michael I. Shamos

A. Dr. Shamos Lacks Qualifications as a Computer Security Expert:

898. While Dr. Shamos may have a Ph.D. in computer science, he has a very thin publication history, and those publications are not particularly germane to any matters related to this case. The subjects of his published articles range from the piezoelectric effect in bone, mathematics, intellectual property law, worker's compensation, and academic titles. Absent from this extensive list is even a single publication about computer security. (Exs. D-20, D-21.)

899. While Dr. Shamos lists five books on his resume, four of them are merely different translations of the same book, a textbook on computational geometry, a field generally associated with computer graphics. (Testimony of Michael I. Shamos ("Shamos Test."), March 23, 2009 Trial Tr. at 63:9-13.) The other book is merely a directory of academic titles used at Carnegie Mellon University. (Shamos Test., 3/23 Trial Tr. at 63:16-24.)

900. While Dr. Shamos has some sparse writings on the subject of voting, he admits that these are mostly about the history of voting, rather than current practice. (Shamos Test., 3/23 Trial Tr. at 73:20-23.) He has written no books on computer security or on voting. (Shamos Test., 3/23 Trial Tr. at 64:14-16, 73:24 to 74:3.) His papers about voting mostly consist of papers delivered at conferences, not peer reviewed publications. (Ex. D-20.)

901. Despite a thirty-four year affiliation with Carnegie Mellon University, he is not a tenured professor at the institution, and is only adjunct faculty. (Shamos Test., 3/23 Trial Tr. at 60:19-61:3.) During most of his affiliation with the University, he has not been engaged in scientific research in the field of computer science.

Instead, he has practiced law, written dozens of articles and books on billiards, and claims to have performed a study on the meaning of the word "about."[24] (Shamos Test., 3/23 Trial Tr. at 61:1-5, 68:6-11.)

902. Dr. Shamos does not advise any Ph.D. students. (Shamos Test., 3/23 Trial Tr. at 62:13-14.)

903. The last awards Professor Shamos won in the field of computer science, are from twenty and thirty years ago, which is eons in the rapidly evolving field of computer science. (Testimony of Michael I. Shamos ("Shamos Test."), March 24, 2009 Trial Tr. at 69:8-13.) He has contributed little to the development of the field since then. The only awards he has since then, have been in fields such as law, billcards, and billiards and bagpipes. (Shamos Test., 3/23 Trial Tr. at 69:14-23.)

B. Dr. Shamos is Biased and has a Personal Financial Stake in Sequoia's Financial Health

904. Dr. Shamos testified that he performs his expert witness work through a company called Expert Engagements, LLC, a company that he and his wife own. (Shamos Test., 3/24 Trial Tr. at 71:16-23.) He is performing his work in this lawsuit through Expert Engagements, LLC. (Shamos Test., 3/24 Trial Tr. at 87:3.)

905. Dr. Shamos testified that 90 percent of what is paid to Expert Engagements is paid to him. (Shamos Test., 3/23 Trial Tr. at 72:11-12.) The remaining 10 percent

[24] Michael Ian Shamos, The New Illustrated Encyclopedia of Billiards (2d ed., Globe Pequot, 1999.)

goes into a joint account shared by Dr. Shamos and his wife. (Shamos Test., 3/23 Trial Tr. at 72:13-14.)

906. Dr. Shamos testified that he is the only expert witness employed by Expert Engagements. (Shamos Test., 3/24 Trial Tr. at 89:5.)

907. Dr. Shamos testified that Sequoia became involved in this case only after he became involved in this case. (Shamos Test., 3/24 Trial Tr. at 86:19-20.),

908. Dr. Shamos was retained by Sequoia's patent counsel in connection with a prior lawsuit - Avante International Technology v. Sequoia Voting Systems, et al. (Shamos Test., 3/24 Trial Tr. at 89:6-11.)

909. Dr. Shamos testified that, at the time of his deposition in this lawsuit, November 24, 2008, he had worked between 300 to 350 hours on behalf of Sequoia on its patent case. (Shamos Test., 3/24 Trial Tr. at 90:1-3.) Dr. Shamos testified that he worked an additional 100 hours on Sequoia's patent case between the time of his deposition and the time he testified at trial in this case. (Shamos Test., 3/24 Trial Tr. at 92:13-14.)

910. Dr. Shamos testified that he was paid $525 an hour for his work on behalf of Sequoia for the patent litigation for a total of between $209,000 and $236,500. (Shamos Test., 3/24 Trial Tr. at 94:18-22.)

911. Dr. Shamos testified that he was hired by Sequoia's patent counsel to participate in another patent suit by Avante against Sequoia. (Shamos Test., 3/24 Trial Tr. at 95:2-11.) Dr. Shamos testified that he expects he will be hired by Sequoia's counsel for a third patent lawsuit. (Id.)

912. Dr. Shamos testified that he expects to write expert witness reports for Sequoia in both additional suits. (Shamos Test., 3/24 Trial Tr. at 95:16.)

913. Dr. Shamos testified he would most likely spend the same amount of time as he has spent working for Sequoia in the original Avante International Technology v. Sequoia Voting Systems, et al suit (450 hours) for Sequoia in each of the additional lawsuits. (Shamos Test., 3/24 Trial Tr. at 96:5-7.)

914. Dr. Shamos expects to charge Sequoia $525 an hour for his services. (Shamos Test., 3/24 Trial Tr. at 90:17-19.) Thus, Dr. Shamos expects to be paid at least another $236,250 from Sequoia for each case, for a total of at least $472,500. (Shamos Test., Trial Tr. at 25:25 to 26:6.)

C. Dr. Shamos Did Not Issue Any Opinions on the Legally Significant Issues in this Case, Even Though He was Paid $73,500 for His Work in this Case

915. Dr. Shamos spent 140 hours working as an expert witness for the State of New Jersey in the DRE lawsuit recently tried before this Court. (Shamos Test., 3/24 Trial Tr. at 101:12 to 102:2.) Dr. Shamos was paid $525 an hour for his work in this lawsuit. (Shamos Test., Trial Tr. at 103:3-17.) The State paid Dr. Shamos approximately $73,500 for his work in this case. (Shamos Test., 3/24 Trial Tr. at 102:12.)

916. Dr. Shamos testified that no one from the Attorney General's Office approached him to ask him about rendering an opinion on the security and reliability of the Sequoia Advantage 9.00H DRE. (Shamos Test., 3/24 Trial Tr. at 106:8-12.)

917. Thus, Dr. Shamos did not offer an opinion on the security and reliability of the Sequoia Advantage 9.00H DRE. (Shamos Test., 3/24 Trial Tr. at 104:25 to

105:8.) Indeed, Dr. Shamos was barred by the Court from offering such an opinion. (Shamos Test., 3/24 Trial Tr. at 105:4-8.)

918. Dr. Shamos does not know what security measures are used in New Jersey, and testified that the security measures in New Jersey are in flux. (Shamos Test., 3/24 Trial Tr. at 69:2-4.)

919. In the 140 hours Dr. Shamos spent working on this lawsuit on behalf of the State, Dr. Shamos did not test the AVC Advantage 9.00H, whose constitutionality and continued use are at issue in this case. (Shamos Test., 3/24 Trial Tr. at 102:21 to 103:15.)

920. In the 140 hours Dr. Shamos spent working this lawsuit, he spent only one hour with the AVC Advantage 9.00H DRE. (Shamos Test., 3/24 Trial Tr. at 103:10-12.) He could not recall the details of what he did, other than to verify that "the option switch bug" actually functioned as discussed in Professor Appel's Expert Report. (Shamos Test., 3/24 Trial Tr. at 103:10-12.)

921. In the 140 hours Dr. Shamos spent working on this lawsuit on behalf of the State, Dr. Shamos did not run any tests on the Sequoia AVC Advantage 9.00H. (Shamos Test., 3/24 Trial Tr. at 103:10-12) He described his interaction with the DRE by saying he merely "exercised the machine so that I could see the effect of the option switch bug." (Shamos Test., 3/24 Trial Tr. at 103:10-12, 104:18-20.)

922. In the 140 hours Dr. Shamos spent working on this lawsuit on behalf of the State, Dr. Shamos did not examine or test the source code or firmware of the Sequoia AVC Advantage 9.00H. (Shamos Test., 3/24 Trial Tr. at 104:13-17, 103:21-24)

923. In the 140 hours Dr. Shamos spent working on this lawsuit on behalf of the State, Dr. Shamos did not examine the hardware of the Sequoia AVC Advantage 9.00H. (Shamos Test., 3/24 Trial Tr. at 103:21-24.)

924. In the 140 hours Dr. Shamos spent working on this lawsuit on behalf of the State, Dr. Shamos did not research New Jersey's proposed security seals. (Shamos Test., 3/24 Trial Tr. at 120:13-18.)

925. In the 140 hours Dr. Shamos spent working on this lawsuit on behalf of the State, Dr. Shamos did not research whether New Jersey's Title 19 Committee certified the Sequoia AVC Advantage 9.00H. (Shamos Test., 3/23 Trial Tr. at 193:23 to 194:3.)

D. Dr. Shamos is the Only Expert Who Supports Voting Systems That Cannot Be Independently Audited by Paper Ballots

926. Dr. Shamos is a staunch supporter of paperless voting systems. (Shamos Test., 3/23 Trial Tr. at 70:4-16.) He has testified numerous times, both before Congress and in connection with lawsuits, in support of paperless voting systems but has never testified in favor of voter verified paper ballots. (Id.)

927. When asked if he could identify any other computer scientists and computer security experts who agreed with his position that paperless DREs are superior to DREs that produce a voter verified paper ballot, Dr. Shamos named two individuals who might agree with this position. (Shamos Test., 3/24 Trial Tr. at 83:8 to 84:17.)

928. Professor Ted Selker of Massachusetts Institute of Technology was one of the experts that Dr. Shamos claimed supported his view on paperless DREs. (Shamos Test., 3/24 Trial Tr. at 83:25.) When confronted on cross-examination with an

article written by Professor Selker lauding optical-scan voting systems, Dr. Shamos admitted that Professor Selker supports software independence, precinct based optical scanners, and that Professor Selker does not support paperless DREs. (Shamos Test., 3/24 Trial Tr. at 109:20 to 110:3.)

929. Professor Juan Gilbert was the other person that Dr. Shamos testified supported paperless DREs. (Shamos Test., 3/24 Trial Tr. at 83:25.) But, Dr. Shamos admitted that Professor Gilbert's own invention, the Prime III voting machine, uses a software independent voter verified paper audit trail. (Shamos Test., 3/24 Trial Tr. at 113:4-7.)

E. Dr. Shamos Fundamentally Agrees with Dr. Appel's Conclusions

930. Dr. Shamos agrees that Professor Appel's examination of New Jersey's DREs is integral to making New Jersey voting machines safer. (Testimony of Michael Shamos ("Shamos Test."), March 25, 2009 Trial Tr. at 10:2-6.)

931. Dr. Shamos testified that "everybody in the voting field should be concerned about Professor Appel's findings." (Shamos Test., 3/25 Trial Tr. at 9:22-23.)

932. Dr. Shamos agrees with Professor Appel that there are problems both with the voting software and the physical security of the Sequoia Advantage 9.00H, and that the AVC Advantage has "serious vulnerabilities." (Shamos Test., 3/23 Trial Tr. at 95:12-15.)

933. Dr. Shamos agrees with Professor Appel that the AVC Advantage has design flaws that allow it to be hacked. (Shamos Test., 3/23 Trial Tr. at 147:16-20.)

934. Dr. Shamos agrees with Professor Appel that the insecurities in the Advantage need to be remedied. (Shamos Test., 3/25 Trial Tr. at 10: 12-25.)

935. Dr. Shamos agrees with Professor Appel that fraudulent firmware can steal votes. (Shamos Test., 3/23 Trial Tr. at 135:6-21.)

936. Dr. Shamos agrees with Professor Appel that by placing fraudulent software in the Sequoia AVC Advantage 9.00H DRE, the DRE can be made to alter election results, and produce fake election results. (Shamos Test., 3/23 Trial Tr. at 112:4-6.)

937. Dr. Shamos agrees with Professor Appel that a vote-stealing program can be created to steal votes for every election after it has been installed on the AVC Advantage 9.00H. (Shamos Test., 3/25 Trial Tr. at 7:8-14.)

938. Dr. Shamos agrees with Professor Appel that a person with ordinary computer training could create a vote-stealing program for a Sequoia AVC Advantage DRE. (Shamos Test., 3/23 Trial Tr. at 136:7-12.)

939. Dr. Shamos agrees with Professor Appel that a vote-stealing program can be created that is undetectable. (Shamos Test., 3/23 Trial Tr. at 130:16-17.)

940. Dr. Shamos agrees with Professor Appel that it is possible to alter all of the ways that the AVC Advantage records and reports election results. (Shamos Test., 3/25 Trial Tr. at 144:12-18.)

941. Dr. Shamos agrees with Professor Appel that replacing a legitimate ROM chip with a fraudulent chip makes the AVC Advantage inaccurate. (Shamos Test., 3/25 Trial Tr. at 143:11-16.)

942. Dr. Shamos agrees with Professor Appel that it is possible for an unauthorized person to replace the ROM chip in the AVC Advantage. (Shamos Test., 3/23 Trial Tr. at 113:1-5.)

943. Dr. Shamos agrees that corrupt poll wokers can install vote-stealing firmware in the Sequoia AVC Advantage 9.00H DRE. (Shamos Test., 3/23 Trial Tr. at 116:1-9.)

944. Dr. Shamos agrees with Professor Appel that no commercially available or certified device exists to test ROM chips to see if their election software is legitimate. (Shamos Test., 3/25 Trial Tr. at 21:15-25; Shamos Test., 3/23 Trial Tr. at 143:4-5, 142:22-24.)

945. Dr. Shamos agrees with Professor Appel that in New Jersey there is no test to determine that the firmware in the AVC Advantage is legitimate. (Shamos Test., 3/25 Trial Tr. at 14:6-17.)

946. Dr. Shamos agrees with Professor Appel that ROM chips are not tested in New Jersey. (Shamos Test., 3/25 Trial Tr. at 19:5-8.)

947. Dr. Shamos agrees with Professor Appel that ROM chips should never be removed from the DREs to validate DRE firmware. (Shamos Test., 3/25 Trial Tr. at 19:5-8.)

948. Dr. Shamos agrees with Professor Appel that if a ROM chip is removed from a suspicious DRE there is no way to determine that the ROM chip that was actually tested was from the suspicious DRE. (Shamos Test., 3/25 Trial Tr. at 21:15-25.)

949. Dr. Shamos agrees that a ROM chip reader could re-write the ROM's firmware. Dr. Shamos agrees with Professor Appel that an attacker using a ROM chip reader to install fraudulent firmware would look no different than a legitimate ROM chip reader. (Shamos Test., 3/24 Trial Tr. at 76:23-25, 77:3-13.)

950. Dr. Shamos agrees with Professor Appel that an insider could replace a real ROM chip with a fake chip. (Shamos Test., 3/24 Trial Tr. at 119:12-16.) Dr. Shamos believes that "Insiders," that is, individuals who have access to voting machines by virtue of their employment, pose the greatest threat to election security because they have the unique ability to tamper with the DREs without having to defeat all of the security mechanisms that are in place to prevent such tampering. (Shamos Test., 3/23 Trial Tr. at 116:1-7; Ex. D-21 at ¶ 89.)

951. Dr. Shamos agrees with Dr. Appel that the AVC Advantage could be tampered with in a warehouse before or after an election. (Shamos Test., 3/24 Trial Tr. at 169:2-6.)

952. Dr. Shamos agrees with Professor Appel that attackers have the opportunity to hack New Jersey's DREs before elections. (Shamos Test., 3/23 Trial Tr. at 136:23 to 137:8.)

953. Dr. Shamos agrees with Professor Appel that an insider could copy a real ROM chip with a ROM chip reader, in a matter of seconds. (Shamos Test., 3/24 Trial Tr. at 119:24 to 120:1.)

954. Dr. Shamos agrees with Professor Appel that an attacker could acquire all of the source code to create fraudulent software from the copied ROM chip. (Shamos Test., 3/24 Trial Tr. at 120:2-4.)

955. Dr. Shamos agrees with Professor Appel that it is possible to reverse engineer ROM chips that are used in the AVC Advantage to create vote stealing programs. (Shamos Test., 3/23 Trial Tr. at 122:4-7.)

956. Dr. Shamos agrees with Professor Appel that an attacker could reverse engineer the source code from the comforts of his own home. (Shamos Test., 3/24 Trial Tr. at 120:5-9.)

957. Dr. Shamos agrees with Professor Appel that an attacker could install a fake Z80 microprocessor in a Sequoia AVC Advantage 9.00H to make the DRE alter the election results. (Shamos Test., 3/25 Trial Tr. at 143:11-16.)

958. Dr. Shamos agrees with Professor Appel that a fake Z80 chip could be manufactured to contain fraudulent firmware that could alter elections. (Shamos Test., 3/25 Trial Tr. at 142:9-16)

959. Dr. Shamos agrees with Professor Appel that people have created computer programs to simulate Z80 processors on hardware that is not an actual Z80. (Shamos Test., 3/25 Trial Tr. at 159:15-21.)

960. Dr. Shamos agrees with Professor Appel that removing the Z80 is not the appropriate way to check if the software on it is fraudulent. (Shamos Test., 3/25 Trial Tr. at 18:12-14.)

961. Dr. Shamos agrees with Professor Appel that the daughterboard can be used to alter votes of blind voters. (Shamos Test., 3/25 Trial Tr. at 35:1-7.) Dr. Shamos agrees with Professor Appel that this problem needs to be remedied immediately. (Shamos Test., 3/25 Trial Tr. at 35:4-7.)

962. Dr. Shamos agrees with Professor Appel that the firmware that reads the audio ballot cartridge needs to be modified. (Shamos Test., 3/25 Trial Tr. at 35:4-7.)

963. Dr. Shamos agrees that the buffer overflow of the audio ballot cartridge allows for election tampering, (Shamos Test., 3/25 Trial Tr. at 35:19 to 36:2), and that the

buffer-overflow bug needs to be fixed immediately. (Shamos Test., 3/25 Trial Tr. at 36:8-14.)

964. Dr. Shamos agrees with Professor Appel that the Sequoia AVC Advantage DRE cannot detect if it has been altered and contains fraudulent firmware. (Shamos Test., 3/25 Trial Tr. at 51:3-6.)

965. Dr. Shamos agrees with Professor Appel that a person who can gain access to WinEDS can alter the AVC Advantage's election results. (Shamos Test., 3/25 Trial Tr. at 33:25 to 34:1.)

966. Dr. Shamos agrees with Professor Appel that WinEDS computers should never be connected to the Internet because Internet connections create security vulnerabilities. (Shamos Test., 3/23 Trial Tr. at 153:22 to 154:2.)

967. Dr. Shamos agrees with Professor Appel that the AVC Advantage can be completely shut down by an attacker who transmits a computer virus, without the attacker ever having physical contact with the DRE. (Shamos Test., 3/23 Trial Tr. at 151:14 to 152:12.)

968. Dr. Shamos agrees with Professor Appel that Sequoia's software development designs for AVC Advantage 9.00H were poor. (Shamos Test., 3/24 Trial Tr. at 171:1-13.)

969. Dr. Shamos agrees with Professor Appel that the AVC Advantage 9.00H does not adequately inform a voter that the DRE has been activated. (Shamos Test., 3/25 Trial Tr. at 37:3-10.) Dr. Shamos agrees with Professor Appel that this can lead to voters to believe they are voting, when instead they are interacting with an unactivated DRE and their vote will be cast but not counted. (Id.)

970. Dr. Shamos agrees with Professor Appel that the AVC Advantage does not communicate with the voter if the voter has undervoted. (Shamos Test., 3/25 Trial Tr. at 39:7-11.)

971. Dr. Shamos agrees with Professor Appel that the "option switch bug" has disenfranchised voters, and that a poll woker could exploit the "option switch bug" to purposely disenfranchise voters. (Shamos Test., 3/25 Trial Tr. at 37:24 to 38:21.)

972. Dr. Shamos agrees with Professor Appel that the AVC Advantage DRE does not allow a voter to edit their write-in vote, nor does it allow a voter to undo a write-in vote. (Shamos Test., 3/25 Trial Tr. at 47:8 to 48:23.)

973. Dr. Shamos agrees with Professor Appel that New Jersey's DRE testing procedure is inadequate for detecting security flaws. (Shamos Test., 3/23 Trial Tr. at 188:4-17.)

974. Dr. Shamos agrees with Professor Appel that if a new computer component, like a daughterboard or microprocessor, is added to a DRE, the whole DRE would need to be re-certified. (Shamos Test., 3/23 Trial Tr. at 203:5-24.) Dr. Shamos agrees with Professor Appel that because one version of a DRE is certified does not mean that any subsequent versions of the DRE are also certified. (Shamos Test., 3/23 Trial Tr. at 206:11-14.)

975. Dr. Shamos agrees with Professor Appel that examiners should spend days on the certification process. (Shamos Test., 3/23 Trial Tr. at 207:8-20.)

976. Dr. Shamos testified each Title 19 Committee member should be "familiar with the computer architectures that are used in these systems. Somebody who is

familiar with security vulnerabilities of computer systems. Basically somebody who can take the manual for these machines and understand what's going on, what the software is doing." (Shamos Test., 3/25 Trial Tr. at 167:25 to 168:6.)

977. Dr. Shamos agrees with Professor Appel that software needs to be examined for security flaws during the certification process. (Shamos Test., 3/25 Trial Tr. at 36:14-16.)

978. Dr. Shamos agrees with Professor Appel that DREs should be examined by computer security experts during the certification process. (Shamos Test., 3/25 Trial Tr. at 49:9-23.)

979. Independent Testing Authorities ("ITAs") came into use following the issuance of the FEC's 1990 guidelines regarding DREs. (Shamos Test., 3/23 Trial Tr. at 103:10-13.)

980. Under these 1990 guidelines, the National Association of State Election Directors established a program that certified ITAs. (Shamos Test., 3/23 Trial Tr. at 103:14-17.)

981. Generally, DRE vendors must obtain reports from ITAs for a state certification process. (Shamos Test., 3/23 Trial Tr. at 103:17-20.)

982. When testing DREs, ITAs follow FEC guidelines. (Shamos Test., 3/23 Trial Tr. at 103:6.)

983. The 1990 guidelines were made more stringent in 2002 and 2005. (Shamos Test., 3/23 Trial Tr. at 178:3-12, 199:17-21.)

984. The FEC guidelines are voluntary. (Shamos Test., 3/23 Trial Tr. at 102:11-13.)

985. Most states have adopted the 2005 guidelines. (Shamos Test., 3/23 Trial Tr. at 184:20.)

986. The State of New Jersey has not adopted the 1990, 2002, or 2005 FEC guidelines. (Shamos Test., 3/23 Trial Tr. at 182:17-18.)

987. New Jersey law does not require DREs to be tested by ITAs. (Shamos Test., 3/23 Trial Tr. at 76:4.)

988. Dr. Shamos agrees with Professor Appel that New Jersey has not adopted the FEC standards for DREs. (Shamos Test., 3/23 Trial Tr. at 182:14-18.) Dr. Shamos agrees with Professor Appel that New Jersey should adopt stronger security guidelines for examining the State's DREs. (Shamos Test., 3/23 Trial Tr. at 187:2-3.)

989. Dr. Shamos agrees with Professor Appel that the ITA tests are ineffective. (Shamos Test., 3/23 Trial Tr. at 187:15-17.)

990. Dr. Shamos testified that ITAs do not test DREs for all possible software flaws that might lead to security weaknesses. (Shamos Test., 3/25 Trial Tr. at 54:7-21.)

991. Dr. Shamos testified that ITAs do not perform enough tests to address DREs security flaws. (Shamos Test., 3/23 Trial Tr. at 190:8-12.)

992. Dr. Shamos testified that ITAs frequently approve DREs that are not qualified to be used in an election. (Shamos Test., 3/23 Trial Tr. at 188:4-17.)

993. ITAs failed to identify the option switch bug in the Sequoia DREs. (Shamos Test., 3/24 Trial Tr. at 116:1-7.) Additionally, the Title 19 Committee and Sequoia failed to identify this bug. (Id.)

994. ITAs failed to identify the buffer overflow bug in the Sequoia DREs. (Shamos Test., 3/24 Trial Tr. at 118:13-22.) The Title 19 Committee and Sequoia also failed to identify this bug. (Id.)

995. The Sequoia DREs have only been tested by ITAs for compliance with the FEC's 1990 guidelines. (Shamos Test., 3/23 Trial Tr. at 182:9-13.)

996. Dr. Shamos has critized ITA reports for many years. (Shamos Test., 3/23 Trial Tr. at 187:22-25.) Importantly, Dr. Shamos believes ITA reports are ineffective, arcane, and deficient. (Shamos Test., 3/23 Trial Tr. at 187:14-15, 187:19; Shamos Test., 3/25 Trial Tr. at 165:19.) In a 2004 Congressional hearing, Dr. Shamos demanded that a new federal voting machine testing system be created from scratch. (Shamos Test., 3/23 Trial Tr. at 189:13-17.)

997. ITAs are not federal agencies. (Shamos Test., 3/23 Trial Tr. at 188:3.)

998. ITAs are paid by vendors. (Shamos Test., 3/23 Trial Tr. at 191:9-10.)

999. Under the 1990 FEC guidelines, vendors can choose the ITA that will test their DREs. (Shamos Test., 3/23 Trial Tr. at 191:18-23.) In choosing ITAs, vendors create an incentive for ITAs to satisfy vendors rather than the public. (Shamos Test., 3/23 Trial Tr. at 192:2-5.) Dr. Shamos believes the process of ITA compensation creates public suspicion. (Shamos Test., 3/23 Trial Tr. at 168:2-7.) Furthermore, he believes that the testing process should be more open. (Id.)

1000. Guidelines established subsequent to the 1990 FEC guidelines have transitioned from using ITAs to using Voting System Testing Laboratories ("VSTLs") certified by the National Institute of Standards and Technology laboratory qualifying program. (Shamos Test., 3/25 Trial Tr. at 151:3-6, 149:5-10.)

1001. Any modification to a DRE can potentially trigger the re-certification process and, consequently, expose an updated DRE to the more recent and rigorous guidelines. (Shamos Test., 3/24 Trial Tr. at 62:1-2.) Consequently, vendors have an incentive to avoid installing vital patches and fixes to known problems to avoid triggering the re-certification process. (Shamos Test., 3/24 Trial Tr. at 150:12-14.)

1002. ITAs do not test the systems of installation, implementation, and utilization of DREs. (Shamos Test., 3/25 Trial Tr. at 167:3-13; Shamos Test., 3/23 Trial Tr. at 188:15-17.)

1003. The Federal Election Commission's 1990 standards do not require an examination of a DRE's software and source code to determine if it is flawed. (Shamos Test., 3/23 Trial Tr. at 192:9 to 193:4.)

1004. Dr. Shamos conceded that VSTLs are still not performing adequately. (Shamos Test., 3/23 Trial Tr. at 190:20.)

1005. Although VSTLs are not chosen by the vendors, they are paid by the vendors. (Shamos Test., 3/23 Trial Tr. at 191:12-14, 191:22-23.)

1006. ITAs and VSTLs test solely within the FEC guidelines. (Shamos Test., 3/23 Trial Tr. at 167:5-6, 167:19-20, 188:14-15.)

1007. Should a bug be discovered or a calamity occur during testing that does not relate to the violation of a guideline, the ITA does not have to report this occurrence. (Shamos Test., 3/23 Trial Tr. at 167:14-20.)

1008. ITAs and VSTLs do not require anti-virus software on DREs or the computers that are utilized in conjunction with DREs. (Shamos Test., 3/23 Trial Tr. at 179:16-19.)

1009. Even the most stringent guidelines – the 2005 FEC guidelines – do not test for software flaws that would lead to security weaknesses. (Shamos Test., 3/25 Trial Tr. at 54:110-11.)

1010. The 1990 guidelines do not require an ITA to examine a DRE's source code. (Shamos Test., 3/25 Trial Tr. at 192:2-4.) Furthermore, members of the Title 19 Committee are not required by law to examine the source code of a DRE. (Shamos Test., 3/25 Trial Tr. at 76:8.)

1011. The 2002 and 2005 guidelines require examination of a DRE's source code, but the examination is limited to known bugs. (Shamos Test., 3/25 Trial Tr. at 199:9-11; Shamos Test., 3/23 Trial Tr. at 155:11-13.)

1012. The ITAs only test known security vulnerabilities. (Shamos Test., 3/25 Trial Tr. at 55:14-16.)

1013. Dr. Shamos agrees with Professor Appel that the Sequoia Advantage 9.00H has not been tested under the 2002 or 2005 FEC standards. (Shamos Test., 3/23 Trial Tr. at 182:6-13.)

1014. As an advisor in Pennsylvania election machine certification, Dr. Shamos performed additional tests on DREs that had passed ITA tests because he believed that ITAs pass too many machines that should have failed. (Shamos Test., 3/23 Trial Tr. at 209:16-21.)

1015. Dr. Shamos agrees with Professor Appel that "the option switch bug is bad." (Shamos Test., 3/25 Trial Tr. at 37:19-23.)

1016. Dr. Shamos agrees with Professor Appel that if a DRE passes FEC standards does not mean that it is secure from computer viruses. (Shamos Test., 3/23 Trial Tr. at 178:17 to 179:12.)

1017. Dr. Shamos agrees with Professor Appel that New Jersey needs to perform tests on DREs in addition to those performed by the ITAs, because the ITAs do not test for all security flaws. (Shamos Test., 3/23 Trial Tr. at 190:8-12.)

1018. Dr. Shamos testified that the principle threat security experts worry about is how insiders can manipulate elections, because insiders do not have to defeat any physical security placed on the voting machine. (Shamos Test., 3/24 Trial Tr. at 114:21 to 115:4, 116:1-3, 116:1-14, 117:24 to 118:2; Shamos Report ¶ 89 ("[i]t is of course important to institute procedures to ensure that [] insiders cannot mount the attacks proposed, or to ensure that any intrusion will be detected.")).

F. Testing Methods Advocated by Dr. Shamos Do Not Exist or Have Never Been Tested

1019. None of the theoretical testing methods proposed by Dr. Shamos for detecting fraudulent software exist or have ever been tested. All computer security experts favor software independence and precinct based optical scanners to Dr. Shamos theoretical testing methods:

1. Parallel Testing

1020. Dr. Shamos testified that he developed parallel testing as a joke. (Shamos Test., 3/24 Trial Tr. at 27:19.)

1021. Parallel testing requires sequestering a DRE during an actual election, and voting on it with a scripted voting pattern throughout the day. Then, after the election,

the DRE is checked to see if the votes recorded by the DRE match the votes identified by the script. (Shamos Test., 3/24 Trial Tr. at 33:13 to 24:7.)

1022. Dr. Shamos testified that parallel testing is based upon following the patterns of voters. (Shamos Test., 3/24 Trial Tr. at 156:7.) Yet, Dr. Shamos also testified that no one knows how to determine the patterns of voters. (Shamos Test., 3/24 Trial Tr. at 155:24 to 156:3.)

1023. Dr. Shamos has never used parallel testing to test the security and reliability of any voting machine. (Shamos Test., 3/24 Trial Tr. at 28:20-24.)

1024. Dr. Shamos testified that he did not use parallel testing to attempt to detect Professor Appel's fraudulent firmware, despite the fact that: he claimed that parallel testing could detect that fraudulent firmware, (Shamos Report, ¶ 50, at 219), and even though he had access to a copy of Professor Appel's fraudulent firmware to conduct parallel testing. (Shamos Test., 3/24 Trial Tr. at 26:11-19.)

1025. Dr. Shamos is aware that parallel testing is currently not used in New Jersey. (Shamos Test., 3/24 Trial Tr. at 122:22-23.) Dr. Shamos has never investigated whether or not New Jersey could use parallel testing successfully. (Shamos Test., 3/24 Trial Tr., at 28:25 to 29:4.)

1026. Dr. Shamos is unaware of any jurisdiction that uses parallel testing in the way he envisions it and devised it. (Shamos Test., 3/24 Trial Tr. at 29:11 to 30:13.)

1027. Dr. Shamos testified that additional DREs would have to be purchased by New Jersey in order to implement parallel testing. (Shamos Test., 3/24 Trial Tr. at 41:15.) Thus, New Jersey would have to spend an unspecified amount of money in order to implement parallel testing. (Id.)

1028. Dr. Shamos testified that New Jersey would have to train workers in order to be able to perform parallel testing. (Shamos Test., 3/24 Trial Tr. at 42:3.)

1029. Dr. Shamos testified that there is no community of experts that advocates for parallel testing. (Shamos Test., 3/24 Trial Tr. at 30:14-17.)

1030. Dr. Shamos testified that there is no organized parallel testing society that advocates for its use. (Id.)

1031. Dr. Shamos testified that there are no academic journal articles in support of parallel testing. (See Shamos Test., 3/24 Trial Tr. at 32:3-6.)

1032. Dr. Shamos admits that all the experts who have commented on parallel testing prefer software independence and precinct-based optical-scan voting machines over parallel testing. (Shamos Test., 3/24 Trial Tr. at 83:25 to 85:1)

1033. Dr. Shamos admitted that none of the individuals whom he claims support parallel testing advocate for it over software independence and precinct-based optical scanners that count paper ballots. (Shamos Test., 3/25 Trial Tr. at 137:11-16.)[25]

2. Checkpointing

1034. Dr. Shamos testified that he invented the process of checkpointing. (Shamos Test., 3/24 Trial Tr. at 50:12.)

1035. Dr. Shamos wrote in his Expert Report that checkpointing could detect Dr. Appel's fraudulent software. (Shamos Report, ¶¶ 50-51.) Yet, Dr. Shamos

[25] In his rebuttal testimony, Professor Appel testified that he actually spoke to the individuals whom Dr. Shamos stated supported parallel testing and that all of them stated that parallel testing was inferior to software independence, DREs with voter-verified paper audit trails, and precinct-based optical scanners. (Appel Test., 4/14 Trial Tr. at 26:17-21.) Professor Appel read the conclusion of the Brennan Center for Justice report to the Court that parallel testing was an inadequate and inferior method for protecting the integrity and accuracy of elections and voting machines. (Appel Test., 4/14 Trial Tr. at 28:18 to 29:10; Ex. P-75.)

testified that he never used checkpointing to determine whether it could detect Dr. Appel's fraudulent firmware. (Shamos Test., 3/24 Trial Tr. at 50:23 to 51:2.)

1036. Dr. Shamos testified that no voting machine exists that can perform checkpointing. (Shamos Test., 3/24 Trial Tr. at 54:11-12.)

1037. Dr. Shamos testified that he would be surprised if any jurisdiction used checkpointing, because checkpointing is very expensive, a "real pain" and an "administrative nightmare." (Shamos Test., 3/24 Trial Tr. at 50:17, 146:9-17.)

1038. Dr. Shamos testified that to perform checkpointing "in a practical election setting would be a real pain." (Shamos Test., 3/23 Trial Tr. at 146:9-10.)

1039. Dr. Shamos testified that the Sequoia AVC Advantage 9.00H cannot even perform checkpointing because it is currently not equipped to do so. (Shamos Test., 3/24 Trial Tr. at 52:16-23.) Sequoia would need to create a completely new DRE with both new hardware and software for checkpointing to be performed. (Shamos Test., 3/24 Trial Tr. at 53:1.)

1040. A new DRE that could perform checkpointing would need to go through a rigorous certification process before it could be used. (Shamos Test., 3/24 Trial Tr. at 53:2-3.)

1041. Election workers would need to be trained to perform checkpointing. (Shamos Test., 3/24 Trial Tr. at 53:15-16.)

1042. New personnel would have to be hired to do checkpointing on Election Day. (Shamos Test., 3/24 Trial Tr. at 53:20.)

1043. Dr. Shamos does not refute Dr. Appel's assertion that a vote-stealing program can avoid and defeat checkpointing. (Appel Test., 1/28 Trial Tr. at 93:21 to 94:20.)

1044. Dr. Shamos testified that checkpointing involves forcing voters to endure longer lines because checkpointing requires a "test voter" cutting into a line of real voters to cast five test votes throughout Election Day. (Shamos Test., 3/24 Trial Tr. at 55:2-6.)

3. The Prime III Voting Machine

1045. Dr. Shamos wrote in his Expert Report that the Prime III would be able to detect Appel's fraudulent firmware. (Shamos Report, ¶ 43.)

1046. The Prime III is not a commercially available product. (Shamos Test., 3/24 Trial Tr. at 56:21-22.) The Prime III is still in the experimental phase. (Shamos Test., 3/24 Trial Tr. at 56:20-21.)

1047. Dr. Shamos testified that the Prime III is a DRE with a touch screen. (Shamos Test., 3/23 Trial Tr. at 163:5-10.) A voter votes on a screen "like a TV" and the Prime III records a picture of the ballot on a DVD. (Shamos Test., 3/23 Trial Tr. at 163:16-20.) Dr. Shamos testified that the software that records the ballot image is completely independent of the software that records the election results. (Shamos Test., 3/23 Trial Tr. at 164:3-7.)

1048. Dr. Shamos does not recommend that New Jersey adopt the Prime III voting system. (Shamos Test., 3/24 Trial Tr. at 56:17-19.)

1049. Dr. Shamos testified that the Prime III has not been certified anywhere. (Shamos Test., 3/24 Trial Tr. at 56:12.)

1050. Dr. Shamos testified that he only used the Prime III once, during a demonstration. (Shamos Test., 3/24 Trial Tr. at 57:1-12.)

1051. Dr. Shamos admitted that the Prime III uses a software independent paper ballot audit trail. (Shamos Test., 3/24 Trial Tr. at 114:3-15.)

XIII. Testimony of John J. Fleming

1052. John J. Fleming serves on the Title 19 Voting Machine Certification Committee as part of his work with the Attorney General's office. (Testimony of John J. Fleming ("Fleming Test.") Apr. 1, 2009 Trial Tr. at 23: 17-21.)

1053. Mr. Fleming was originally listed as a witness for Defendants. He did not testify for Defendants and Plaintiffs called him as a rebuttal witness. His testimony was severely limited.

1054. Mr. Fleming has no formal computer security training and is not a computer security expert. Mr. Fleming only has knowledge of the operating systems that he works on at the Attorney General's office, and those computer systems are not voting machines. (Fleming Test., 4/1 Trial Tr. at 41:8-18.)

1055. Mr. Fleming did not receive any training before becoming a member of the Title 19 Committee. (Fleming Test., 4/1 Trial Tr. at 24:12-17.)

1056. As a member of the Title 19 Committee, Mr. Fleming was not given any materials to interpret Title 19. (Fleming Test., 4/1 Trial Tr. at 25 at 1-3.)

1057. Other than relying on ITA reports, the Title 19 Committee does not do anything to ensure that the voting machines presented by vendors comply with New Jersey law concerning accuracy and reliability. (Fleming Test., 4/1 Trial Tr. at 29:10-15.)

1058. On average, the Title 19 Committee spends 15 minutes discussing a vendor's presentation after a hearing. (Fleming Test., 4/1 Trial Tr. at 31:10-17, 33:18 to 34:9, 35:1-9.)

1059. Certification presentations by the vendors have been done remotely when the Title 19 Committee is not present in the room. (Fleming Test., 4/1 Trial Tr. at 30:13-22.)

1060. These certification presentations have been done by teleconference, where the Title 19 Committee would not be able to physically examine voting machines or the DREs. (Fleming Test., 4/1 Trial Tr. at 30:13-25.)

XIV. Testimony of Plaintiffs' Expert Dr. Roger Johnston

A. The State's Approach To Physical Security Reflects The Lack Of A Healthy Security Culture, Without Which New Jersey Will Be Unable To Implement Effective Seal-Based Security

1061. The Court heard extensive testimony about the poor physical security of New Jersey's DREs from Plaintiffs' expert witness Dr. Roger Johnston, a Senior Systems Engineer at Argonne National Laboratories. (Testimony of Roger Johnston ("Johnston Test."), Apr. 21, 2009 Trial Tr. at 11:7-11; see also Expert Report of Roger G. Johnston, Docket No. MER-L-2691-04, pp. 47-59 (hereinafter "Johnston Expert Report"), Ex. P-81.) Dr. Johnston earned his MA and Ph.D. in physics from the University of Colorado in 1983. (Johnston Test., 4/21 Trial Tr. at 12:12-14.)

1062. Argonne is a federal national laboratory owned by the Department of Energy, and run by the University of Chicago. (Johnston Test., 4/21 Trial Tr. at 11:7-11.) Dr. Johnston is Section Manager of Argonne's Vulnerability Assessment Team, which examines security devices, systems, and programs, identifies flaws, and recommends countermeasures. (Johnston Test., 4/21 Trial Tr. at 15:4-14.) His team at Argonne works on projects with sensitive national security implications, including nuclear safeguards and security applications. (Johnston Test., 4/21 Trial Tr. at 16:8-10.) Dr. Johnston's work has made him one of the world's preeminent experts on security seals. (See Johnston Expert Report, at 47.)

1063. Dr. Johnston's expertise also extends to evaluating security culture. Security culture is the formal and informal approaches to security that an organization must adopt in order to implement effective security. (Johnston Test., 4/21 Trial Tr. at 18:11-23.)

1064. Over the past twenty years, Dr. Johnston has studied hundreds of kinds of security seals, and published over 115 articles on seals and security in industry publications. (Johnston Test., 4/21 Trial Tr. at 20:11-14.) He is Editor of the Journal of Physical Security (Johnston Expert Report, at 49), the first scholarly, peer-reviewed journal devoted exclusively to physical security research and development.[26] He holds a US government Top Secret Q clearance, allowing him to study seals used on nuclear safeguards and other sensitive national-security applications. (Johnston Test., 4/21 Trial Tr. at 11:14-12:4.)

1065. Before working at Argonne, Dr. Johnston founded the Los Alamos National Laboratories Vulnerability Assessment Team, and spent fifteen years as its Team Leader. (Johnston Expert Report, ¶ 4.) Los Alamos, like Argonne, is a federal national laboratory owned by the Department of Energy. (Johnston Test., 4/21 Trial Tr. at 13:25-14:1.) At Los Alamos, Dr. Johnston worked on projects involving homeland security, nuclear safeguards and nonproliferation compliance, counter-terrorism, biophysics, chemistry, and laser applications, in addition to security seals and tamper detection. (Johnston Expert Report, at 46.) His projects were sponsored by the International Atomic Energy Agency, the European Atomic Energy Community (Euratom), among others. (Id.) He has consulted for the Department of Energy, the Department of Defense, the Nuclear Regulatory Commission, the National Institutes of Health, and numerous private corporations. (Johnston Test., 4/21 Trial Tr. at 49.)

---

[26] http://jps.anl.gov/

1066. Dr. Johnston has won numerous awards. His awards at Los Alamos included a Fellows Prize for Outstanding Research, two Distinguished Service Awards, three Achievement Awards, the Award for Student Mentoring, and two awards for Excellence in Technology Transfer. (Johnston Expert Report, at 47.) He won a Distinguished Performance Award from the Central Intelligence Agency in 2002. (Id.)

1067. Dr. Johnston was a Science Fellow at the Center for International Security and Cooperation at Stanford University from 2000-2001. Johnston Expert Report, at 46. Between 1983 and 1985 he was a postdoctoral fellow at Los Alamos. (Id.) He also won the Carver Physics Fellowship and the Tozer Foundation Graduate Student Scholarship. (Johnston Test., 4/21 Trial Tr. at 27:19-20.)

1068. Ross Anderson, Professor of Security Research at Cambridge University, has written "the most impressive physical security research team in the world is probably Roger Johnston's Vulnerability Assessment Team." (Johnston Expert Report, at 47.)

1069. Dr. Johnston has also earned a Certified Protection Professional certificate from the American Society for Industrial Certification (ASIS), which requires years of experience in the field, comprehensive examination, and regular demonstrations of professional growth. (Johnston Test., 4/21 Trial Tr. at 13:1-14.) He holds ten patents, with one more patent application currently pending. (Johnston Expert Report, at 47.)

1070. Dr. Johnston received no remuneration from Plaintiffs for the expert services he performed on Plaintiffs' behalf. (Johnston Test., 4/23 Trial Tr. at 121:15-17; Johnston Test., 4/24 Trial Tr. at 111:6-18.)

1071. In its Rule 104 Hearing of April 21, the Court certified Dr. Johnston to give expert testimony on everything covered by the Expert Report he submitted, along with its addendum. (Johnston Test., 4/21 Trial Tr. at 49:24 to 50:4.) Under the Court's certification, Dr. Johnston's expertise covered all aspects of physical security, including security seals, security culture, physical vulnerabilities, attacks on seals, inspections, backdoor attacks, DRE storage, and background checks. (Johnston Test., 4/21 Trial Tr. at 47:1 to 48:25.)

1072. The State never called any witnesses with any expertise in physical security. Thus, Dr. Johnston's testimony is the only testimony before the Court on the subject of physical security as it relates to New Jersey's DREs. His conclusions – that New Jersey has no security culture, and that the State's proposed seals can be defeated without detection – are uncontested by any expert or evidence.

B. The State's Proposed Seals Cannot Provide Effective Security for the State's 11,000 DREs, because New Jersey's has No Security Culture

1073. Dr. Johnston testified that "one can't have good security no matter how good the hardware if one doesn't have a good security culture." (Johnston Test., 4/21 Trial Tr. at 19:2-6.) An organization with a healthy security culture, according to Dr. Johnston, builds security into everything it does, at every level: it engages in critical self-review; approaches security proactively; incorporates a desire to improve security into every level of the organization, (Id.); and eagerly solicits input on security from all quarters, both internal and external. (Johnston Test.,

4/21 Trial Tr. at 57:19 to 58:4.) It does not wait passively for security problems to be pointed out by an external agent, (Johnston Test., 4/21 Trial Tr. at 57:9-16), or respond in an ad hoc way to vulnerabilities by "slapping on" some third-party solution. (Johnston Test., 4/21 Trial Tr. at 58:3.) Indeed, as Dr. Johnston testified, a healthy security culture regards security not as a commodity for sale, but as an ongoing process integral to all operations. (Id.)

1074. Dr. Johnston concluded that New Jersey suffers from an unhealthy security culture with regard to its DREs, making elections conducted on the DREs vulnerable to numerous attacks.

C. An Example Of The State's Poor Security Culture Is That It Has Introduced Numerous Security Seals, Many After The Trial Started, Without Crafting Any Use Protocols For Applying and Inspecting The Seals

1075. Perhaps no better indication of New Jersey's unhealthy security culture exists than its approach to security seals on the eve of trial and during trial. Dr. Johnston examined no fewer than thirteen seals since he became involved in this case in 2009. (Johnston Test., 4/21 Trial Tr. at 78:20.) All of the seals were introduced after the discovery phase had already ended. (Id.)

1076. The State did not consult any independent security experts before introducing security seals. (Johnston Test., 4/21 Trial Tr. at 79:7-10.) Additionally, the State has changed its seals in response to advice gleaned from Plaintiffs' expert testimony; a reactive, rather than a proactive, approach. (Id.) The State's ad hoc measures leave the DREs open to multiple attacks. (Johnston Expert Report, ¶ 64.)

1077. The State began introducing its security seals in November 2008, two months before trial was to begin. This was many months after Professor Appel

demonstrated that the Sequoia Advantage 9.00H DRE could be hacked to steal votes in less than 7 minutes by replacing the DRE's legitimate ROM chip with a fraudulent one. (Certification of Professor Andrew Appel, ¶ 5, Dec. 1, 2008, Docket No. MER-L-2691-04.) Since November 2008, New Jersey has introduced twelve new security seals:

- Plastic Strap Seal---no evidence was provided by the State on how long these seals have been used. Of the two DREs given to Professor Appel to examine, only one had a Plastic Strap Seal installed.

  November 13, 2008[27]

  1. Red Adhesive Tape with New Jersey State seal[28]
  2. Wire Cable Lock Seal[29]
  3. Large Cup Seal
  4. Blue Plastic Strap Seal

  December, 2008

  5. Blue Plastic Strap Seal
  6. Small Brooks MRS2 Pressure-Sensitive Seal[30] (The State has represented that it wishes to produce this seal with ultra violet markings. Such a seal does not yet exist. Notwithstanding, Dr. Johnston discussed the ultra violet markings in his Expert Report and in his testimony.)
  7. Large Brooks MRS2 Pressure-Sensitive Seal
  8. Brooks Padlock Seal
  9. Small Cup "Seal"

  April 9, 2009

  10. Small Cup "Seal" with Gorilla Glue

---

[27] Certification of Professor Andrew Appel, ¶ 5, Dec. 1, 2008, Docket No. MER-L-2691-04.

[28] The security markers in this seal are covered by the protective order, and will be discussed in a later section of this submission that will be redacted from the public version of this submission.

[29] The State has made multiple representations to the Court that this seal was no longer being contemplated for use.

[30] The security markers in this seal are covered by the protective order, and will be discussed in a later section of this submission that will be redacted from the public version of this submission.

11. Large Cup Seal with Gorilla Glue
12. Brooks Red Adhesive Tape Seal

1078. The State's poorly planned and hasty introduction, withdrawal, and re-introduction of seals has not made the State's DREs safer in any way. (Johnston Test., 4/21 Trial Tr. at 79:25 to 80:5.) Dr. Johnston's opinion is that New Jersey, like other "organizations with poorly thought-through security pile[s] on multiple security features, devices, or layers in hopes that the complex interaction of all these layers will somehow automatically add up to good security." (Johnston Expert Report, ¶ 95; Johnston Test., 4/21 Trial Tr. at 166:18-25.) He testified, further, that it takes at least several months per seal of intensive work and training to develop effective seal use protocols. (Johnston Test., 4/21 Trial Tr. at 79:18-24.)

D. The State Proposes To Cover Deep, Inherent Security Flaws For Its DREs By Using A Superficial "Band-Aid" Approach

1079. The sheer number of seals proposed by the State demonstrates its lack of a coherent security policy for New Jersey's DREs. (Testimony of Roger Johnston ("Johnston Test."), Apr. 22, 2009 Trial Tr. at 120:24-25.) New Jersey proposes to use six different seals in nine locations on its DREs. (Johnston Test., 4/22 Trial Tr. at 119:17-19.)

1080. Dr. Johnston testified that in seventeen years at the forefront of his field, he has never seen so many seals used at once, including on top-secret nuclear safeguards and other high-level national-security applications. (Johnston Test., 4/21 Trial Tr. at 120:2-7.) The most seals he has ever seen in one application were three. (Johnston Test., 4/21 Trial Tr. at 120:14-16.)

1081. This is because in order to have effective security systems, security professionals consciously minimize the complexity of their programs. (Johnston Test., 4/21 Trial Tr. at 120:16-21.) Each new seal added to a system multiplies the complexity of the use protocols necessary to ensure its effectiveness. (Id.) As Dr. Johnston testified, "with security, as with many things in life, simplicity is the best approach." (Johnston Test., 4/21 Trial Tr. at 121:10-11.) Complexity, on the other hand, both compounds the cost of a security program, (Johnston Test., 4/21 Trial Tr. at 120:1-2), and introduces new vulnerabilities. (Johnston Test., 4/21 Trial Tr. at 120:24-25.)

1082. Dr. Johnston concluded that the unprecedented complexity of New Jersey's seals will overwhelm seal inspectors, as they struggle to do a good job on every seal under a more and more minutely detailed rubric. (Johnston Test., 4/21 Trial Tr. at 121:2-9.)

E. New Jersey Has Not Established Protocols Governing The Use Of Its Proposed Seals, And Therefore Cannot Use Them Effectively

1083. Dr. Johnston testified that "a seal is . . . no better than its use protocol." (Johnston Test., 4/21 Trial Tr. at 81:6-7.) New Jersey has taken no steps to establish use protocols for its proposed seals. Without protocols, the proposed seals cannot fulfill their most basic security function.

1084. New Jersey currently has no protocols in place governing how it will use its proposed security seals. (Johnston Test., 4/21 Trial Tr. at 80:9.) Without rigorous protocols governing every aspect of their use, the proposed security seals will not provide effective security. (Johnston Test., 4/21 Trial Tr. at 80:13-16.) Seal use protocols should govern seals "from cradle to grave," including how they are

chosen, procured, used, transported, installed, inspected, removed, disposed of, how training is done, who the personnel are, and so on. (Johnston Test., 4/21 Trial Tr. at 80:23-24.)

1085. The reason for establishing use protocols is that tamper-indicating seals are only as effective as they are predictable. (Johnston Test., 4/21 Trial Tr. at 174:14-23.) Seal inspectors must know how a seal is supposed to look and behave in order to inspect it. (Johnston Test., 4/21 Trial Tr. at 101:2-13.) For seals to look and behave predictably, they must be installed, handled, and inspected in a consistent way. (Id.)

1086. Dr. Johnston concluded that New Jersey's lack of any security protocols gravely compromises election security. First, New Jersey has no protocol governing proposed seal installations. Seals, according to Dr. Johnston, often suffer incidental damage, such as inadvertent scratches or dents, during installation. (Johnston Test., 4/21 Trial Tr. at 22:1 to 23:3.) No protocol exists in New Jersey either ensuring consistent installation techniques or directing personnel to take notice of incidental damage inflicted during installation. (Id.) A seal inspector confronted with a damaged seal, but with no way to discern whether the damage is evidence of tampering or merely incidental, has no sound basis to determine whether or not an attack has taken place. (Id.) As a result, election security suffers.

1087. New Jersey also has no protocols in place for *inspecting* seals. Because the essential function of seals is to detect tampering, seals are only as effective as the inspection protocols in place. Indeed, it is fair to say that the only function of

seals is *to be inspected.* Effective inspections take account of the unique properties and vulnerabilities of each particular seal; in order for that to happen, they must be governed by carefully thought-out protocols.

F. The State Administers Elections Without Consulting Any Professional Security Experts, Resulting In Systemic Vulnerabilities

1088. Dr. Johnston testified that in developing a healthy security culture, it is essential to seek advice from on-staff and external security experts. (Johnston Test., 4/21 Trial Tr. at 60:1-9.) New Jersey has no on-staff security experts, and has consulted no physical security experts. (Johnston Test., 4/21 Trial Tr. at 60:19-22.) Instead, the State has relied exclusively upon the manufacturers of the seals for security advice, particularly the Brooks Company. (Johnston Test., 4/21 Trial Tr. at 60:1-10.) The conflict of interest should be obvious: a seal manufacturer has a financial interest in selling seals. This does not take into account the security interests of its clients. (Id.) Indeed, seals that Mr. Giles testified were recommended by Brooks as being foolproof were defeated by both Dr. Johnston and Professor Appel. (See, e.g., Johnston Expert Report, ¶ 106.)

G. Mr. Giles Fails To Understand Security Generally, And Is Unaware Of Important Aspects Of New Jersey's Election Security, Creating Further Vulnerabilities For New Jersey's DREs

1089. According to Dr. Johnston, the fact that Mr. Giles, the Director of the Division of Elections, does not understand physical or cyber security illustrates New Jersey's poor security culture. (See Johnston Test., 4/21 Trial Tr. at 58:5 to 64:3.) Dr. Johnston's Expert Reports emphasize that security depends crucially on organizational security culture and priorities. (See Johnston Expert Report, ¶ 36.) As Director of the Division of Elections, Mr. Giles' own attitudes and

understanding have a tremendous affect on New Jersey's election security. (Johnston Expert Report, ¶ 62.)

1090. After reading Mr. Giles' deposition, Dr. Johnston concluded that "[i]n my professional opinion, Mr. Giles' views represent major barriers to having good election integrity, and show evidence of an unhealthy security culture." (Id.) Dr. Johnston identified numerous, basic misunderstandings of security in Mr. Giles' deposition, demonstrating that Mr. Giles lacks the crucial expertise needed to secure New Jersey's DREs.

- Mr. Giles testified that he has not consulted any independent security professionals about New Jersey's DREs. (Johnston Test., 4/21 Trial Tr. at 60:1 to 62:5; Johnston Expert Report, ¶ 67, citing Giles Deposition, Jan. 6, 2009, at 36-37 (hereinafter "Giles Dep.)) Dr. Johnston testified that it is essential to work with outside, independent security professionals in order to build a strong security culture. (Johnston Test., 4/21 Trial Tr. at 60:1-22.) Further, he testified that Mr. Giles must hire internal security professionals in order to build an effective program. (Id.) The fact that he has not, Dr. Johnston concluded, shows a total lack of a systematic approach to security. (Id.) Although DRE security depends critically on security culture, Mr. Giles has taken no steps to obtain reliable information about security.
- Mr. Giles criticized Professor Appel's reported attacks on the security seals because one videotaped attempt allegedly did not succeed. (Johnston Test., 4/21 Trial Tr. at 62:22 to 63:5; Johnston Expert Report, ¶ 74, citing Giles Dep., 199-200.) As Dr. Johnston testified, taking a vulnerability seriously only after it has been demonstrated to perfection makes it impossible to be proactive, a core aspect of healthy security culture. (Johnston Test., 4/21 Trial Tr. at 57:1-6, 73:24-74:11.) Dr. Johnston reports that Mr. Giles' attitude is "backwards from how an effective security program and healthy security culture operates." (Johnston Expert Report, ¶ 81.) Dr. Johnston reported that under Mr. Giles' leadership, New Jersey will "have great difficulty providing good security, or developing a healthy security culture." (Id. ¶ 75.)

- Mr. Giles testified that the only advice he sought on security seals was from representatives of Brooks Security Company, a seal vendor whose goal is to sell its products. (Johnston Test., 4/21 Trial Tr. at 60:1-9; Johnston Expert Report, ¶ 77, citing Giles Dep., 208-09.) Dr. Johnston reported that objective and independent guidance is critical, especially for users like Mr. Giles, who do not understand security. (Johnston Test., 4/21 Trial Tr. at 60:13-15; Johnston Expert Report, ¶ 77.) A vendor is ultimately interested in its bottom line, not in its customers' security programs. (Johnston Test., 4/21 Trial Tr. at 62:8-10.)

- Mr. Giles testified that the State plans to leave its proposed security seals on the DREs at all times. (Johnston Expert Report, ¶ 78, citing Giles Dep., 224:25.) Dr. Johnston concluded that this policy creates four serious security problems:

  (a) The seals cannot be thoroughly inspected because they will not be removed for close visual examination. (Johnston Expert Report, ¶ 78; see also Johnston Test., 4/21 Trial Tr. at 174:9 to 176:5.)

  (b) The single most effective way to inspect an adhesive tape seal, like the MRS seal or the Brooks Red Tape Seal, is to *remove* it and observe its behavior. (Id.)

  (c) Without removing the seals, inspectors are unable to access the internal electronics. (Id.) Dr. Johnston has demonstrated several electronic attacks on the DREs that cannot be detected without close inspection of the inner circuitry. (See, e.g., Johnston Expert Report, ¶¶ 144-53.)

  (d) Without removing the seals, inspectors are unable to inspect the seals on the Z80 microprocessor or the EPROMS in the DREs. (Id.) ¶ 78.

In other words, according to Mr. Giles, New Jersey has no plans to inspect its seals or its DREs on a regular basis.

- Mr. Giles testified that cheating in a single election for one candidate is not a matter of concern. (Johnston Expert Report, ¶ 69, citing Giles Deposition, at 90, 253-54.) Dr. Johnston concludes in his report that the idea that election fraud is acceptable so long as it is limited in scope is

diametrically opposed to proactive thinking about security. (Id.)

1091. Dr. Johnston identified numerous statements made by Mr. Giles demonstrating Mr. Giles's lack of knowledge about security issues and even of the State's DREs:

- Mr. Giles testified that New Jersey does not test its machines for hackability. (Johnston Test., 4/21 Trial Tr. at 72:4-23; Johnston Expert Report, ¶ 72, citing Giles Dep. at 194-95.)
- Mr. Giles testified that a hacker would need the DRE's source code in order to reverse engineer the firmware. (Johnston Expert Report, ¶ 70,citing Giles Dep. at 92-94.) This is simply wrong. (Johnston Expert Report, ¶ 70; see also (Johnston Test., 4/21 Trial Tr. at 62:18-20.)
- Mr. Giles testified that altering the firmware on a DRE would not dramatically affect its functionality. (Johnston Expert Report, ¶ 66, citing Giles Dep., 36-37.) This is simply wrong. (Johnston Expert Report, ¶ 66.)
- Mr. Giles testified that New Jersey has "put a security seal on a tamper evident piece of tape." (Johnston Test., 4/21 Trial Tr. at 63:9-14; Johnston Expert Report, ¶ 71, citing Giles Dep. at 192.) Mr. Giles does not even understand proper security terminology and concepts. As Dr. Johnston explains, the piece of tape is the seal. (Johnston Expert Report, ¶ 71.) Without understanding the seal, Mr. Giles cannot use it effectively. (Johnston Test., 4/21 Trial Tr. at 63:16-20.)

1092. Mr. Giles does not know about New Jersey's DRE testing, does not know about the DREs themselves, does not know about computer security, and does not know about physical security. Without understanding his own programs, Mr. Giles will not be able to develop an effective security program. (Johnston Expert Report, ¶ 62.)

1093. Dr. Johnston identified even more indicators or poor security culture in New Jersey by examining the depositions of James Clayton of Ocean County, Elisa Gentile of Hudson County, and Daryl Mahoney of Bergen County. (Johnston

Test., 4/21 Trial Tr. at 67-69.) He laid special emphasis on security vulnerabilities in the transport, storage, and delivery of DREs.

- DREs are left unsecured at polling places for up to two weeks at a time. (Johnston Test., 4/21 Trial Tr. at 67:14-21; see also Johnston Expert Report, ¶ 86, citing Clayton Deposition, at 66-68.)
- Counties choose companies to transport DREs with no attention to security, (Johnston Test., 4/21 Trial Tr. at 68:1-8), and with no background checks. (Id. at 68:18-25, citing Mahoney Deposition, at 32-36, 58-60, and Gentile Deposition, at 63-67, 89-91, 93-95.)
- The keys to each DRE are kept with the machine in the warehouse, where temporary workers are allowed to interact with them without background checks. (Johnston Expert Report, ¶ 89, citing Mahoney Deposition, at 58-60; see also Johnston Test., 4/21 Trial Tr. at 67:23 to 68:8.)
- There is no documentation or formal chain of custody for the transport, delivery, and acceptance of DREs at polling places. (Johnston Test., 4/21 Trial Tr. at 67:1-11; Johnston Expert Report, ¶ 92, citing Gentile Deposition, at 91, 93-95.)

1094. These flaws create genuine security vulnerabilities. On the basis of his research, and after reading the depositions cited, Dr. Johnston concluded that:

> [g]iven limited security features built into the AVC Advantage voting machine, the absence of a healthy security culture for New Jersey elections, and New Jersey's lack of well designed seal use protocols, I believe there are viable attacks on New Jersey voting machines that are . . . capable of affecting election results.

(Johnston Expert Report, ¶ 93; see also Johnston Test., 4/21 Trial Tr. at 58:19-21.) New Jersey's poor security culture creates the possibility that an election may be stolen.

1095. Dr. Johnston characterized New Jersey as suffering from a phenomenon called "cognitive dissonance:" the tendency of officials who want to have good security to deny evidence of security vulnerabilities, and to be unwilling to consider

potential programs or proactively seek them out. (Johnston Test., 4/21 Trial Tr. at 73:10-23.) Dr. Johnston testified about objective research demonstrating that a poor attitude toward security results in vulnerabilities. (Johnston Test., 4/21 Trial Tr. at 75:11-24.) Dr. Johnston has published articles in industrial/organizational psychology journals on cognitive dissonance, and has supervised a Ph.D. thesis on the subject. (Johnston Test., 4/21 Trial Tr. at 75:20-24.) He has shown that statistically significant correlations exist indicating that attitudes towards security are powerful predictors of security problems. (Johnston Test., 4/21 Trial Tr. at 75:11-17.) New Jersey's unhealthy security culture, in other words, is itself an indicator that State elections are vulnerable to attack.

H. All of the Seals Proposed by the State Are Readily Defeated With Little Expertise, Money, or Technology

1096. During both direct and cross examination, Dr. Johnston demonstrated to the Court that simple, low-tech, inexpensive methods exist for defeating all of New Jersey's proposed seals. Further, he demonstrated attacks requiring no expertise beyond that of a high-school-age hobbyist. (Addendum to Johnston Expert Report, ¶ 32.)

I. During His Direct Testimony Dr. Johnston Demonstrated the Successful Defeat of All The Security Measures Proposed by the State Demonstrations Before the Court

1097. Dr. Johnston defeated all of the seals contemplated by the State, in open court, despite the fact that the State continued changing its proposed seals as late as April 2009. (See generally Testimony of Roger Johnston ("Johnston Test."), Apr. 23, 2009 Trial Tr. and Apr. 24, 2009 Trial Tr.; see also Addendum to Johnston Expert Report, ¶ 1.) This includes seals provided to him in early 2009, as well as seals that the State proposed for use months after trial began. (See id.) With little

notice, Dr. Johnston devised successful defeats for all of the seals he was given, in a very short time. (Id.)

1098. The attacks Dr. Johnston demonstrated are only the tip of the iceberg. (Johnston Test., 4/21 Trial Tr. at 54:2-13; Johnston Expert Report, ¶ 47.) Dr. Johnston testified that it is essential to take seriously every feasible attack that can be conceived, even if it has not been demonstrated. (Johnston Test., 4/21 Trial Tr. at 54:14-20.) According to Dr. Johnston, security vulnerabilities are unlimited. (Id. at 54:2-4.) Assessing vulnerability, as Dr. Johnston testified, is about identifying the vulnerabilities most likely to be exploited, and addressing those that can be fixed. (Id. at 54:9-13.)

1099. Just as it is crucial to take every conceivable attack seriously, it is crucial to take every possible attacker seriously. An attacker need not have a Ph.D. to devise and successfully implement an attack. (See Johnston Test., 4/22 Trial Tr. at 129:20-24; Johnston Expert Report, ¶ 61.) In fact, Dr. Johnston reported that in his experience, "the average laboratory technician, auto mechanic, artist, crafts person, or wood worker can master attacks on seals more quickly than Ph.D.'s and can demonstrate better mechanical proficiency." (Id.; see also Johnston Test., 4/22 Trial Tr. at 84:22-25.) According to Dr. Johnston, his team of technicians and students at Argonne National Laboratory define attacks as "especially easy" if Dr. Johnston can perform them. (Johnston Expert Report, ¶ 61.)

1100. Dr. Johnston's courtroom demonstrations prove beyond any doubt that it is possible to defeat all of New Jersey's proposed seals. They represent only a small subset of the possible methods for hacking into the State's DREs. (Johnston

Test., 4/21 Trial Tr. at 54:2-13.) Notably, the time it took Dr. Johnston to defeat the seals is not in any way indicative of how long someone with more practice and with good manual dexterity would take to defeat the seals. (Johnston Test., 4/21 Trial Tr. at 144:3-6.)

1. Brooks Blue Padlock Seal

1101. The Brooks Padlock seal is a padlock with three components: a clear plastic housing containing a blue plastic body; and an arched, steel shackle that clips into the blue body just like a padlock shackle. (Johnston Test., 4/21 Trial Tr. at 81:13-22; Exs. P-83 to P-87.) The blue plastic body on each Brooks Padlock Seal is marked with an adhesive label bearing a serial number with a barcode. (Id.) Once the shackle is engaged, it is not supposed to be removable without destroying the seal. (Id.; see also Giles Deposition, 212:19-21.) Dr. Johnston demonstrated two methods for defeating this seal:

1102. Dr. Johnston uses the term "partial counterfeit" to describe this attack, because he uses parts of the real seal to produce the counterfeit. (Johnston Test., 4/21 Trial Tr. at 84:23 to 85:1.)[31]

[31] A full counterfeit, as Dr. Johnston testified, would be produced entirely from fresh materials, without cannibalizing any parts of the real seal. (Johnston Test., Apr. 21, 2009, 84:23 to 85:1.)

[redacted]

1103. Samples of the Brooks Padlock Seal are readily available to the general public. Brooks distributes free samples upon request, and sells large quantities at low cost. (Johnston Test., 4/21 Trial Tr. at 83:24 to 84:2.) As a result, an attacker is easily able to acquire Padlock Seals to dismantle for spare parts or practice attacks. Dismantling the seals is a simple matter; Dr. Johnston testified that an attacker could dismantle seals at his leisure, even while watching TV. (Id. at 88:15-17.)

1104. Another method for defeating the Brooks Padlock Seal is to make a counterfeit seal bearing the same serial number. (Johnston Test., 4/21 Trial Tr. at 90:19 to 91:4.) This method produces a full counterfeit, since no parts of the real seal are used. (Johnston Test., 4/21 Trial Tr. at 84:23 to 85:1.) [redacted]

[redacted]

[redacted]

[redacted]

1105. Dr. Johnston brought seven such counterfeit Padlock Seals with him to court. (Johnston Test., 4/21 Trial Tr. at 91:23 to 92:17.) They were admitted into evidence as Ex. P-88. He was able to manufacture the counterfeits literally on the eve of trial, among all his other preparations, [redacted] He presented the seven counterfeits along with one original, all bearing the same serial number, to the Court and Defendants' counsel for inspection one at a time. (Johnston Test., 4/21 Trial Tr. at 93:15 to 95:17.) Neither the Court nor Defendants' counsel were able to distinguish the genuine seal from the counterfeits, nor one seal from another. (Id.)

1106. Dr. Johnston presented the seals to the Court one at a time in order to simulate actual inspection conditions. (Johnston Test., 4/21 Trial Tr. at 94:1 to 95:17.) In the real world, seal inspectors examine seals one at a time. (Id.) They often work in poor lighting. (Johnston Test., 4/21 Trial Tr. at 162:17-25.) Unlike in the courtroom setting, real inspectors are not given advance warning that a seal has been counterfeited, and thus may lack motivation. (Johnston Test., 4/21 Trial Tr. at 94:1 to 95:17.) They do not have a counterfeit and a legitimate seal to compare during inspections, but must evaluate only what is before them. (Id.)

1107. Moreover, seal inspections cannot be effective in an unhealthy security culture. (Johnston Test., 4/21 Trial Tr. at 75:11-17.) Detecting a counterfeit is practically impossible without detailed protocols structured to address the specific vulnerabilities of the seal. (Johnston Test., 4/21 Trial Tr. at 97:20-24.) Unless seals are inspected under carefully conceived protocols, according to Dr. Johnston, an attacker could steal votes without being detected. (Johnston Test., 4/21 Trial Tr. at 81:11-12.) As Dr. Johnston put it, given New Jersey's nonexistent use protocols, "the most minimal of effort will constitute a defeat." (Id.)

2. Brooks Padlock Seal With Gorilla Glue

1108. After learning of Dr. Appel's success defeating the Brooks Padlock Seal in December 2008, the State proposed adding Gorilla Glue to the seal. The State proposes to inject the Gorilla Glue into the hole where the shackle engages, on the theory that the glue will hold the seal together, preventing the kinds of simple defeats identified by Dr. Johnston. (Johnston Test., 4/21 Trial Tr. at 100:7-10.)

1109. Dr. Johnston was easily able to defeat the glued Brooks Padlock Seal. It was a simple matter of producing a counterfeit as described above (see section II.A.1), and then adding Gorilla Glue before engaging the shackle. (Johnston Test., 4/21 Trial Tr. at 105:8 to 106:11.) In Dr. Johnston's terminology, this is a full counterfeit, as it is made entirely from fresh materials. (Johnston Test., 4/21 Trial Tr. at 84:23 to 85:1.) Dr. Johnston successfully produced glued counterfeits in Court, (Johnston Test., 4/21 Trial Tr. at 105:8 to 106:11), which were admitted into evidence as Ex. P-89. He testified that adding the Gorilla Glue has the

opposite effect of what Defendants intended. It makes the seals less secure. (Johnston Test., 4/21 Trial Tr. at 100:20 to 101:1.)

1110. The Gorilla Glue leaves marks on the Brooks Padlock Seals that, in Dr. Johnston's opinion, are likely to lead inspectors to make incorrect determinations. (Johnston Test., 4/21 Trial Tr. at 103:5 to 104:18.) When the Gorilla Glue is injected into the clear plastic housing and the shackle is engaged, it flows throughout the clear plastic housing and across the serial number label in unpredictable patterns. (Johnston Test., 4/21 Trial Tr. at 100:20 to 101:1; Ex. P-89.) As noted above, the key to tamper-indicating seals is predictability. (Johnston Test., 4/21 Trial Tr. at 174:14-23.) The glue flow patterns make every seal look different in ways that are meaningless to inspectors unless a photograph is taken of every single seal. (Johnston Test., 4/21 Trial Tr. at 101:2-13.) If the glue is injected in both sides, the random effect is twice as bad. (Johnston Test., 4/21 Trial Tr. at 104:16-18.) The State's poor understanding of the proposal to add Gorilla Glue to the Brooks Padlock Seals illustrates how its unhealthy security culture fails to protect the DREs from attack. (See, e.g., Johnston Test., 4/21 Trial Tr. at 100:7-16) (explaining that the lack of an installation protocol makes the Gorilla Glue useless.)

3. American Casting and Manufacturing Small Cup "Seal"

1111. The American Casting and Manufacturing (ACM) Small Cup Seal is fundamentally a device meant to protect the screws on New Jersey's DREs from being opened with an ordinary screwdriver. (Johnston Test., 4/21 Trial Tr. at 156:7-17.) The Small Cup "Seal" consists of two parts: a cup with a hole in it through which the screw is inserted, (Id.); and a cap that snaps onto the cup. (Id.)

Once the cap is attached, the head of the screw is theoretically inaccessible, supposedly converting the screw into a robust security seal. (Id.)

1112. But, the Small Cup "Seal" is not a seal at all! It lacks any unique identifier, a critical aspect of tamper-indicating seals. (Johnston Test., 4/21 Trial Tr. at 148:11-15.) Additionally, the three-eighths-inch device chosen by New Jersey is no longer manufactured by ACM. (Johnston Test., 4/21 Trial Tr. at 150:3-11.) It does not come engraved with serial numbers. (Id.) Without a serial number, the device lacks any unique identifier, and does not qualify as a tamper-indicating seal under the most basic definition. (Johnston Test., 4/21 Trial Tr. at 148:18-20.) Each and every Small Cup "Seal" is identical, making it impossible to detect a swap. (Johnston Test., 4/21 Trial Tr. at 149:2-8.)

1113. Even if serial numbers are added to the Small Cup "Seals," the serial numbers will be too difficult to read to offer any effective security. (Johnston Test., 4/21 Trial Tr. at 162:17-25.) The Small Cup "Seal" is very small, so the serial number printed on it would necessarily be even smaller. Even under good illumination conditions, Dr. Johnston testified that the numbers will be very difficult read. (Id.) He testified that the location of the seals made the Small Cup "Seals" even harder to read. (Johnston Test., 4/21 Trial Tr. at 163:5 to 167:14.) His conclusion, based on past experience, was that seal inspectors will not do a good job on seals that are difficult to inspect. (Id.) Even if the Small Cup "Seal" were a legitimate tamper-indicating security seal marked with a serial number, they would still not afford effective security.

1114. The fact that ACM no longer manufactures the Small Cup "Seal" renders the device meaningless from a security perspective. The State proposes to install the Small Cup "Seals" in three locations on the DREs: underneath the audio cartridge; on the power panel; and in the upper-left corner of the metal cover. (Johnston Test., 4/21 Trial Tr. at 163:10 to 165:17.)

1115. With 11,000 DREs in use in New Jersey, the State will need to install 33,000 Small Cup "Seals" at the outset. Further, large quantities of the seals are needed as examples to train installers and inspectors. (Johnston Test., 4/21 Trial Tr. at 150:21 to 151:1.) It is also important for inspectors to witness demonstration attacks on real seals, which usually cannot be re-used afterwards. (Johnston Test., 4/21 Trial Tr. at 151:2-9.) All of these activities will diminish the existing supplies of the device. Dr. Johnston had no trouble ordering approximately sixty sample Small Cup "Seals" from ACM, further diminishing the number available to New Jersey. (Johnston Test., 4/21 Trial Tr. at 152:10-22.)

1116. The Small Cup "Seal" can be easily defeated. [redacted]

Dr. Johnston was able to complete the attack within thirty seconds. (Id.) More facile members of his team were able to complete it within three to ten seconds. (Id.) The cost of the attack is negligible given the stakes: [redacted] The attack does not damage the seal, which can be reused,

making the attack all but undetectable. (Johnston Test., 4/21 Trial Tr. at 154:10-15.)

1117. Dr. Johnston is able to defeat the Small Cup "Seals," even if serial numbers are added. (Johnston Test., 4/21 Trial Tr. at 160:16-24.) [redacted]

[redacted]

4. American Casting and Manufacturing Large Cup Seal

1118. In his testimony, Dr. Johnston described two attacks that defeat the Large Cup Seal also manufactured by ACM. Like the Small Cup Seal, the Large Cup Seal comprises a bottom cup and a top cap that snaps on. (Johnston Test., 4/21 Trial Tr. at 168:12-20.) The cap snaps on with "leaf-spring fingers" that hold it in place. (Id.)

1119. Dr. Johnston's first attack is the same as his attack on the Small Cup Seal: [redacted]

[redacted] Dr. Johnston is able to perform this attack within 90 seconds; technicians on his Vulnerability Assessment Team are able to perform it within 10 seconds. (Johnston Test., 4/21 Trial Tr. at 171:10-15.)

1120. In Dr. Johnston's second attack, [redacted]

[redacted]

[redacted]

1121. [redacted]

1122. Both of these attack methods produce partial counterfeits, since parts of the original Cup Seals remain in place. (Johnston Test., 4/21 Trial Tr. at 84:23 to 85:1.)

5. American Casting and Manufacturing Small and Large Cup Seals With Gorilla Glue

1123. The State has also proposed adding Gorilla Glue to the Cup Seals in response to the defeats Professor Appel demonstrated in court and to the defeats discussed in Dr. Johnston's Expert Report. This measure actually made the seal easier for Dr. Johnston to defeat. (Johnston Test., 4/21 Trial Tr. at 172:10-11.)

1124. This new measure is problematic in many ways. In Dr. Johnston's courtroom demonstration (Ex. P-102), the Gorilla Glue stuck the parts of the Cup Seals together. (Johnston Test., 4/21 Trial Tr. at 172:23 to 173:25.) As a result, Dr. Johnston was able to remove the seals like normal screws, simply by turning the whole apparatus, by hand! (Johnston Test., 4/21 Trial Tr. at 188:21 to 195:22.) He glued the top cap of each seal to the bottom cup, attempting not to fill the whole cavity. Although he made every effort to apply the Gorilla Glue consistently, he found that the Gorilla Glue is by its nature unpredictable. (Johnston Test., 4/21 Trial Tr. at 184:6 to 185:4.)

1125. Moreover, the application of the glue itself causes serious problems for inspectors. The Gorilla Glue shrinks as it cures, pulling on the surface of the top cap and causing dimples to appear unpredictably. (Johnston Test., 4/21 Trial Tr. at 186:5-19.) The presence of unpredictable damage on genuine seals makes it easier to mask an actual attack. (Id.)

1126. The glue proposed by the State is a cyanoacrylate, a hazardous chemical with serious environmental and health effects. (Johnston Test., 4/21 Trial Tr. at 179:15-20.) Dr. Johnston consulted the Material Safety and Data Sheet for cyanoacrylates, which states that "[cyanoacrylate adhesive] . . . bonds with human tissue including skin in seconds." Material Safety Data Sheet for Cyanoacrylate Adhesives, available at http://www.elfy.com/TAIGAR/MSDN.htm. Further, when a cyanoacrylate like Gorilla Glue comes in contact with clothing or human tissue, it "will generate heat causing smoke, sun burns and strong irritating vapors." (Id.) Any worker responsible for gluing hundreds of seals would face prolonged exposure. (Id.) New Jersey has not addressed the potential OSHA issues arising from these hazards.

6. Plastic Strap Seals

1127. The State has also introduced a Plastic Strap Seal manufactured by Electek. (Johnston Test., 4/21 Trial Tr. at 138:5.) Dr. Johnston defeated the seal on his first attempt, after spending a mere ten minutes examining it. (Johnston Test., 4/22 Trial Tr. at 115:6-8.) Dr. Johnston has shown how to pick open strap seals with everyday materials, in a matter of seconds. (Johnston Expert Report, ¶ 131.)

1128. The Plastic Strap Seal is based on a ratchet principle: the seal's toothed plastic strap slides into a plastic body, where the teeth engage with a locking mechanism.

(Johnston Test., 4/21 Trial Tr. at 139:22-23.) [redacted] This attack leaves the seal undamaged: an attacker would simply replace the original seal, making the attack undetectable. (Johnston Test., 4/21 Trial Tr. at 144:3.)

1129. Dr. Johnston's [redacted] attack is widely known and discussed among hobbyists on the Internet. (Johnston Test., 4/21 Trial Tr. at 145:8-16.) The only equipment needed to successfully perform the attack is [redacted] (Johnston Test., 4/21 Trial Tr. at 146:5.)

1130. Dr. Johnston was also able to defeat the Plastic Strap Seal using [redacted] (Id.) With little expertise or expense, according to Dr. Johnston, an attacker can defeat the Plastic Strap seals, potentially changing election outcomes.

7. Brooks Red Adhesive Tape Seal Installation Problems

1131. The Red Tape Seal suffers from serious flaws that increase its cost to the State, and its vulnerability to attack. The adhesive substrate is so strong that the seals are very difficult to remove from the rolls on which they are shipped. (Johnston Test., 4/21 Trial Tr. at 199:5-12.) The plastic top layer tends to separate from the substrate on removal from the roll, causing damage to the edges and exposing the "void, opened" marks on the substrate. (Johnston Test., 4/22 Trial Tr. at 52:14-

22.) These damaged seals are irreparable and unusable, resulting in numerous wasted seals at great expense to the taxpayers. (Id.)

1132. Dr. Johnston examined photographs taken by Professor Appel of the Red Tape Seal applied to the DREs. (Ex. P-77.) He testified that the inconsistent installation results inherent to the Red Tape Seal make it easier for attackers to defeat the seals. (Johnston Test., 4/21 Trial Tr. at 205:20 to 207:24.)

1133. For example, the Red Tape Seal leaves marks wherever it is applied, so that if an installer fails to lay the seal down correctly on the first attempt, he will leave a mess of glue around the seal. (Johnston Test., 4/21 Trial Tr. at 202:13 to 205:13.) Dr. Johnston observed this kind of damage in Professor Appel's photograph of the Red Tape Seal on the DRE audio cartridge, which had damage to the upper-left corner and upper edge. (Johnston Test., 4/21 Trial Tr. at 201:19 to 202:6; Ex. P-77, Fig. 23.) He concluded that a close-up of the same Red Tape Seal revealed adhesive on the surface around the seal deposited during the installation process. (Johnston Test., 4/21 Trial Tr. at 202:9-24; Ex. P-77, Fig. 19.)

1134. This kind of damage compromises the efficacy of the seal. The likelihood that seals will appear damaged tends to lead inspectors either to erroneously identify tampering, or to learn to expect damage; Dr. Johnston concludes that these flaws open New Jersey's DREs to attack. (Johnston Test., 4/21 Trial Tr. at 203:20 to 205:19.)

1135. Dr. Johnston also testified that the Red Tape Seal installed on the left side of the DRE had a bubble in the lower-right corner. (Johnston Test., 4/21 Trial Tr. at 205:2-13; Ex. P-77, Fig. 17.) He testified that the bubble could be an indication

of an attack, but in this case was the result of the difficulty of installing the Red Tape Seal. (Johnston Test., 4/21 Trial Tr. at 205:7-13.) In his opinion, the Red Tape Seals, as demonstrated in the photographs taken by Professor Appel would lead to a false positive: an inspector would erroneously report an attack. (Johnston Test., 4/21 Trial Tr. at 205:16.) The occurrence of false positives drastically undercuts the efficacy of a seals program. (Johnston Test., 4/21 Trial Tr. at 206:14-22.) Indeed, inspectors who expect to see routine damage will overlook evidence of an attack. (Id.) The seal that "cries wolf" is not an effective guard.

8. Brooks Red Adhesive Tape Seal Installation Problems

1136. The messiness of the Red Tape Seal also requires time-consuming clean-up, further compromising its efficacy. As discussed earlier, the Red Tape Seal leaves behind its adhesive substrate when removed. But the seal will only adhere correctly to a clean surface. (Johnston Test., 4/22 Trial Tr. at 65:12-14.) Thus, every time a Red Tape Seal is removed, the substrate must be cleaned off before a replacement can be applied. (Id.) When Dr. Johnston demonstrated the cleaning process for the Court, it took him twelve minutes. (Johnston Test., 4/24 Trial Tr. at 138:11-13.)

1137. To clean off the gunk, Dr. Johnston had to use solvents that give off toxic fumes. (Johnston Test., 4/22 Trial Tr. at 63:20 to 64:22.) In fact, when Dr. Johnston was cleaning off the gunk in the courtroom, the court reporter asked and was granted permission to exit the courtroom for the duration of the demonstration, because she could not endure the powerful, toxic fumes. (Johnston Test., 4/24 Trial Tr. at 155:25 to 156:3.) Dr. Johnston testified that the solvent he used causes harm to

health from long-term exposure. (Johnston Test., 4/24 Trial Tr. at 159:23-24; Ex. P-115.) The solvent, which Dr. Johnston testified has much the same effects as other solvents, is labeled with the following warnings:

> Danger: harmful or fatal if swallowed. Contains acetone, xylene, ethyl benzene, butyl carbitol, petroleum distillates, and toluene. Contact physician immediately. Do not induce vomiting. Avoid prolonged contact with skin. Do not get in eyes. In case of eye contact, flush with water for 15 minutes. . . [E]xtremely flammable liquid and vapor. Vapor harmful or fatal if swallowed.

(Johnston Test., 4/24 Trial Tr. at 160:2-12.) Dr. Johnston testified that in order to clean the adhesive from all of its DREs, New Jersey would have to buy dangerous solvents in 55-gallon drums. (Johnston Test., 4/24 Trial Tr. at 161:23 to 162:3.)

1138. Since the State proposes to use the Red Tape Seals in two locations on the DREs, an inspector would have to spend twelve minutes exposed to the fumes for every seal he removed. (Johnston Test. 4/24 Trial Tr. at 157:16-12.) That adds up to twenty-four minutes per DRE. Many counties have hundreds of DREs.

1139. Any maintenance person changing a battery or even checking to see if the EPROMs have been tampered with would suffer the same harmful exposure. (Johnston Test., 4/24 Trial Tr. at 133:11-15.) Workers responsible for removing, inspecting, and installing hundreds or thousands of seals would ultimately spend hundreds of hours exposed to dangerous chemicals, causing serious harm to their health.

1140. After more than seventeen years leading the most respected teams in the field, Dr. Johnston concluded that if it is difficult to inspect a seal, inspectors will not do a thorough job. (Johnston Test., 4/22 Trial Tr. at 166:8-13.) A seal inspector asked

to spend twenty-four minutes per machine cleaning gunk and breathing toxic fumes will not do a good enough job to protect New Jersey's DREs from attack. (Id.)

9. Attack on Brooks Red Pressure-Sensitive Adhesive Tape Seal

1141. The Brooks Red Pressure-Sensitive Adhesive Tape Seal (Red Tape Seal) comprises two parts: an adhesive substrate, and a red plastic top layer. (Johnston Test., 4/22 Trial Tr. at 27:14-19.) The adhesive substrate bears the words "void" and "opened." (Johnston Test., 4/22 Trial Tr. at 58:3-7.) The two words remain behind when the seal's top layer is removed, providing tamper indication. (Id.)

1142. In one corner of the substrate, a unique serial number is printed. (Johnston Test., 4/22 Trial Tr. at 27:14-19.) The plastic top layer has a clear window in the same location through which the serial number is visible. (Id.) But when the plastic top layer is removed, the serial number stays behind on the adhesive substrate. (Johnston Test., 4/22 Trial Tr. at 27:19 to 28:5.)

1143. Exploiting this characteristic, Dr. Johnston demonstrated a straightforward method for defeating the Red Tape Seal:

1144. Since the original serial number remains in place, this attack is a partial counterfeit. (Johnston Test., 4/21 Trial Tr. at 84:23 to 85:1.) The strength of the attack is that the defeated seal behaves just like a normal one; the attack is undetectable without sophisticated chemical forensics. (Johnston Test., 4/21 Trial Tr. at 118:16 to 119:1; see also Johnston Test., 4/24 Trial Tr. at 34:5-8.) The total cost of the equipment for this attack was between $7 and $9, according to Dr. Johnston. (Id. at 62:19 to 63:2.)

10. Brooks Small MRS2 Pressure-Sensitive Adhesive Seal

1145. Dr. Johnston testified that pressure-sensitive adhesive seals like the Small Brooks MRS2 Seal do not provide effective security. (Johnston Test., 4/21 Trial Tr. at 107:7-11; Johnston Expert Report, ¶ 117.) In fact, the Small Brooks MRS2 Seal is "even easier to defeat than many other [pressure-sensitive adhesive] seals." (Johnston Expert Report, ¶ 117.) This is because the seal's adhesive is weak, making it easy to lift off the DRE. (Johnston Test., 4/21 Trial Tr. at 107:13-16; Johnston Expert Report, ¶ 118.)

1146. Dr. Johnston also testified that it is easy to counterfeit the Small Brooks MRS2 Seal using inexpensive, low-tech equipment. (Johnston Test., 4/21 Trial Tr. at 110:22-24.) Each seal has a unique serial number printed on it. (Johnston Expert Report, Fig. 5.) Dr. Johnston uses the following method to produce a full counterfeit:

1147. Dr. Johnston testified that using solvents to attack adhesive-tape seals is a well-known attack method. (Johnston Test., 4/21 Trial Tr. at 114:14-17.) For at least three decades, according to Dr. Johnston, people have been discussing this method of attacking adhesive-tape seals like the Small Brooks MRS2 Seal on the internet. (Johnston Test., 4/21 Trial Tr. at 114:20-23.) Dr. Johnston testified that numerous government reports dating back to the 1970s document the vulnerability of pressure-sensitive adhesive seals to solvents. (Johnston Test., 4/21 Trial Tr. at 114:23 to 115:1.)

1148. This kind of attack is so well known that it only took Dr. Johnston two minutes to figure out how to defeat the Small Brooks MRS2 Seal. (Johnston Test., 4/21 Trial Tr. at 115:5.)

1149. Dr. Johnston testified that it is simple to produce a counterfeit MRS2 serial number. (Johnston Test., 4/21 Trial Tr. at 116:4-8.)

[redacted] The Small Brooks MRS2 Seal has no bar code, making it even easier to produce a full counterfeit. (Johnston Test., 4/21 Trial Tr. at 112:21-22.)

1150. Often, according to Dr. Johnston, one can order specific serial numbers from seal manufacturers. (Johnston Test., 4/21 Trial Tr. at 116:22 to 117:3.) An attacker may be able to order a range of custom serial numbers from Brooks. (Id.) With counterfeits made to order by the manufacturer, an attacker would have an even easier time installing vote-stealing software on New Jersey's DREs. (Id.)

1151. No special expertise is needed to perform this attack. An attacker with access to a [redacted] is fully equipped to produce a full counterfeit. (Johnston Test., 4/21 Trial Tr. at 115:10-17.)

1152. Dr. Johnston brought five counterfeit Small Brooks MRS2 Seals with him to court. (Johnston Test., 4/21 Trial Tr. at 109:3-6.) They were admitted into evidence as Ex. P-90. Like the Brooks Padlock Seal, Dr. Johnston was able to manufacture counterfeit Small Brooks MRS2 Seals on the eve of trial. (Johnston Test., 4/21 Trial Tr. at 109:9-19.) He presented the five counterfeits along with one original, all bearing the same serial number, to the Court and Defendants' counsel for inspection one at a time. (Johnston Test., 4/21 Trial Tr. at 109:20 to 110:8.) Neither the Court nor Defendants' counsel were able to distinguish the genuine seal from the counterfeits, nor one seal from another. (Johnston Test., 4/21 Trial Tr. at 111:8 to 112:9.)

1153. Again, presenting seals to the Court one at a time simulates actual inspection conditions, according to Dr. Johnston. (Johnston Test., 4/21 Trial Tr. at 111:11-

18.) A real seal inspector examines seals one at a time, with no warning that an attack has taken place, and with no opportunity to examine an attacker's different attempts. (Id.)

1154. Dr. Johnston testified further that more high-tech methods exist for defeating the Small Brooks MRS2 Seal. (Johnston Test., 4/21 Trial Tr. at 117:13-18.) For example, the vinyl material that the seal is made of is also used in standard vinyl tape, available at grocery and hardware stores. (Johnston Test., 4/21 Trial Tr. at 117:19-22.) An attacker could use a home hobbyist [redacted] to manufacture a sophisticated counterfeit. (Johnston Test., 4/21 Trial Tr. at 118:9-15.) An advanced attack like this could defeat even a relatively advanced seal use protocol. (Id.) Materials are readily available to make high-quality counterfeits of the Small Brooks MRS2 Seal, making New Jersey's DREs vulnerable to vote-stealing attacks. (Johnston Test., 4/21 Trial Tr. at 118:5-8.)

11. Brooks Large MRS2 Pressure-Sensitive Adhesive Seal

1155. New Jersey also proposes to use a larger version of the Brooks MRS2 Seal. (Johnston Test., 4/21 Trial Tr. at 135:12-14.) Dr. Johnston testified that the Large Brooks MRS2 Seal is fundamentally the same as the Small Brooks MRS2 Seal. (Johnston Test., 4/21 Trial Tr. at 136:7-12.) He testified, further, that he is able to defeat the Large Brooks MRS2 Seal using the same technique as the Small Brooks MRS2 Seal. (Id.) He is able to manufacture a partial counterfeit of the Large Brooks MRS2 Seal using [redacted] (Id.)

1156. Dr. Johnston testified that the Large Brooks MRS2 Seal has a rectangular box printed on it, for seal installers to add their signatures. (Johnston Test., 4/21 Trial

Tr. at 135:17 to 136:5.) New Jersey does not use this feature; it installs the Large Brooke MRS2 Seal without a signature. (Id.) Adding a signature to the seal, according to Dr. Johnston, would make a counterfeiting attack somewhat more complicated. (Id.) Although Dr. Johnston testified that adding a signature would not substantially improve the Large Brooks MRS2 Seal's security, (Id.), and the fact that the State has ignored this feature is further evidence of its poor security culture.

THE FOLLOWING TESTIMONY IS SUBJECT TO THE PROTECTIVE ORDER:

12. Brooks Small MRS2 Pressure-Sensitive Adhesive Seal with Ultraviolet Markings

1157. The Brooks Small MRS2 seal produced by the State does not exist with an ultraviolet mark or logo. (Johnston Test., 4/21 Trial Tr. at 120:14-24.)

1158. Dr. Johnston testified that, to his understanding, Brooks has merely discussed providing the Small MRS2 seal with an ultraviolet mark as an option, but no such seal is currently in production. (Johnston Test., 4/21 Trial Tr. at 120:-21-24.)

1159. Although it is very difficult to assess the viability of a seal that does not exist, (Johnston Test., 4/21 Trial Tr. at 121:1-3), the use of ultraviolet marks or logos is quite common and goes back many decades. (Johnston Test., 4/21 Trial Tr. at 121:13-20.) Indeed, the use of an ultraviolet mark on a seal is "probably the most obvious thing anyone looking at a seal trying to see if there was some anti-counterfeiting feature would think about." (Johnston Test., 4/21 Trial Tr. at 123:16-21.)

1160. Spotting an ultraviolet mark on a seal is as simple as shining an ultraviolet flashlight on the seal. (Johnston Test., 4/21 Trial Tr. at 127:11-24.) By

examining the seals initially for ultraviolet markings, an attacker could decide whether he wanted to counterfeit the marking or whether he wanted to attack the seal in such a way that did not disturb the ultraviolet portion. (Id.)

1161. Counterfeiting an ultraviolet mark is essentially no different than counterfeiting a visible ink mark. (Johnston Test., 4/21 Trial Tr. at 126:3-7, Exs. P-94, P-95, P-96.) All one needs is a rubber stamp and an ultraviolet ink pad. (Johnston Test., 4/21 Trial Tr. at 129:1 to 130:15.) Rubber stamps can be custom made from any art work. (Johnston Test., 4/21 Trial Tr. at 129:14-16.) The Seal of the State of New Jersey is readily available on the State's website. (Johnston Test., 4/21 Trial Tr. at 129:22 to 130:2.)

1162. The materials needed to counterfeit a seal with an ultraviolet logo are readily available to consumers on the Internet. (Johnston Test., 4/21 Trial Tr. at 134:5-22.) Materials include lower cost items such as a rubber stamp and an ink pad, but there are also ultraviolet printer cartridges that go into laser printers that consumers, and attackers, can purchase. (Id.)

1163. An attacker does not have to recreate the logo with precision because one of the advantages (to an attacker) of an ultraviolet image is that it is difficult to see. (Johnston Test., 4/21 Trial Tr. at 130:16-24.) If the ultraviolet image has roughly the same shape and approximately the same fluorescent color, then it will typically be accepted by the seal inspeactor as an indication of the ultraviolet mark, and hence not counterfeit. (Johnston Test., 4/21 Trial Tr. at 130:24 to 131:5.)

1164. The method in which the State proposes to use the ultraviolet seals would assist an attacker. The State proposes to use ultraviolet seals bent across the ROM chips on the motherboard. This makes the seals very difficult to inspect. (Johnston Test., 4/21 Trial Tr. at 132:1-13, 133:10-25.)

1165. Dr. Johnston testified that ultraviolet markings do not represent any significant extra security feature, and do not increase the tamper detection reliability of a seal. (Johnston Test., 4/21 Trial Tr. at 128:4-14, 131:6-8.)

END OF PROTECTED TESTIMONY

J. On Cross Examination Dr. Johnston Again Defeated All of the Security Measures Proposed By The State In Ways That Avoid Detection

1166. On cross examination, Dr. Johnston was asked to defeat all of the seals that were placed by Mr. Giles on the Sequoia AVC Advantage DRE that was in the State's custody. (See generally Johnston Test., 4/24 Trial Tr.) He defeated all of the seals. (Id.)

1167. Dr. Johnston testified at length concerning the poor likelihood that seal inspectors would detect the attacks of New Jersey's proposed seals that he demonstrated. (Johnston Test., 4/24 Trial Tr. at 25:10 to 44:25, 165:3 to 167:2.) At the Court's request, Dr. Johnston testified about three different levels of security protocols, Level 1, Level 2, and Level 3, and when his attacks would be detected using each level of security protocol. (Id.)

1168. Level 1, the level in use in New Jersey, is no seal use protocol, no plan for inspections, and no training on attacks or understanding of attack methods. (Johnston Test., 4/24 Trial Tr. at 25:14-24.)

1169. Level 2 is some kind of seal use protocol, with modest training on the protocol for seal installers and inspectors. (Johnston Test., 4/24 Trial Tr. at 25:25 to 26:2.)

1170. Level 3, the highest level, is a very effective seal use protocol combined with extensive training. (Johnston Test., 4/24 Trial Tr. at 26:3-6.) In reality, implementing Level 3 protocols is so complex and expensive that they are almost never used. (Johnston Test., 4/24 Trial Tr. at 165:24 to 166:14.) Dr. Johnston testified that even nuclear safeguards rarely use Level 3 protocols. (Id.) Further, he testified that his Vulnerability Assessment Team has found it a very difficult challenge to develop Level 3 protocols. (Id.) Forensic lab results of the kind required for Level 3 protocols can take weeks to obtain. (Johnston Test., 4/21 Trial Tr. at 118:20-24.) The extreme cost and complexity of Level 3 protocols makes them all but nonexistent in practical applications. (Johnston Test., 4/24 Trial Tr. at 165:24 to 166:14.)

1171. Dr. Johnston's conclusions about the efficacy of different protocol levels on each seal are as follows:

- Brooks Padlock Seal with Gorilla Glue: Dr. Johnston defeated this seal by making and installing a counterfeit bearing the same serial number as the Brooks Padlock Seal installed on the DRE by the State. (See Johnston Test., 4/21 Trial Tr. at 81:13 to 90:3.) New Jersey currently has no use protocols in place for this seal, putting it at Level 1. (Johnston Test., 4/21 Trial Tr. at 80:9.)

1172. Level 1: Dr. Johnston concluded that without use protocols, an inspector would likely perform a basic visual examination and serial number check. (Johnston Test., 4/24 Trial Tr. at 27:8-16.) This would not detect his attack on the Brooks Padlock Seal with Gorilla Glue, or any comparable attack. (Id.)

1173. Level 2: Level 2 protocols for the Brooks Padlock Seal would likely include more careful visual inspection, and some tactile examination. (Johnston Test., 4/24 Trial Tr. at 28:2-13.) Level 2 protocols would not detect Dr. Johnston's attack on the Brooks Padlock Seal with Gorilla Glue. (Id.)

1174. Level 3: Level 3 protocols would involve disassembling the seal and carefully studying the individual components under a microscope. (Johnston Test., 4/24 Trial Tr. at 28:14-23.) Level 3 would detect an attack. But, according to Dr. Johnston, detection would be extraordinarily expensive. (Id. at 28:25 to 29:4.)

- Large and Small Brooks MRS2 Tape Seals: Dr. Johnston produced a partial counterfeit of the Small Brooks MRS2 Seal. [redacted] (Johnston Test., 4/21 Trial Tr. at 110:22 to 112:22.) Dr. Johnston testified that he defeated the Large Brooks MRS2 Seal using the same method. (Johnston Test., 4/21 Trial Tr. at 135:12 to 136:12.) New Jersey currently has no use protocols in place for the Large or Small Brooks MRS2 Seals, putting it at Level 1. (Johnston Test., 4/21 Trial Tr. at 80:9.)

1175. Level 1: Dr. Johnston concluded that without use protocols, an inspector would likely perform a basic visual examination and serial number check on the Large and Small Brooks MRS2 Seals. (Johnston Test., 4/24 Trial Tr. at 29:15 to 30:6.) This would not detect his attack on the Large or Small MRS2 Seals, or any comparable attack. (Id.)

1176. Level 2: Dr. Johnston testified that at best, Level 2 protocols for the Large and Small Brooks MRS2 Seals would involve outstanding training and highly motivated installers. (Johnston Test., 4/24 Trial Tr. at 30:8-15.) Nonetheless, Dr. Johnston concluded that the odds of detecting his attack on the Large and Small

Brooks MRS2 Seals with Level 2 protocols are at best 50%. (Johnston Test., 4/24 Trial Tr. at 31:12-13.)

1177. Level 3: Even though a Level 3 protocol would detect Dr. Johnston's attack, Level 3 protocols would involve expensive and complex forensic examination of the seal's chemical makeup. (Johnston Test., 4/24 Trial Tr. at 31:16-17.) Such detailed examination is, again, prohibitively complex and costly. (Johnston Test., 4/24 Trial Tr. at 165:24 to 166:14.)

- Brooks Red Adhesive Tape Seal: Dr. Johnston defeated this [redacted] at 27:19 to 28:5, 78:1-9.) New Jersey currently has no use protocols in place for this seal, putting it at Level 1. (Johnston Test., 4/21 Trial Tr. at 80:9.)

1178. Level 1: Dr. Johnston concluded that without use protocols, an inspector would likely perform a basic visual examination and serial number check. (Johnston Test., 4/24 Trial Tr. at 32:25 to 33:20.) This would not detect his attack on the Brooks Red Adhesive Tape Seal, or any comparable attack. (Id.)

1179. Level 2: To qualify as Level 2, protocols would have to devote attention both to the serial number and to any damage inflicted during installation. (Johnston Test., 4/24 Trial Tr. at 33:21 to 34:4.) With careful training and motivated staff, Dr. Johnston testified Level 2 protocols would have a 50% chance of detecting his attack. (Id.)

1180. Level 3: Even though a Level 3 protocol would detect Dr. Johnston's attack, Level 3 protocols would involve disassembling the Brooks Red Tape Seal and analyzing the chemicals on the underside of the tape. (Johnston Test., 4/24 Trial Tr. at 34:5-8.) Performing such detailed analysis on 11,000 DREs would be

prohibitively complex and costly. (Johnston Test., 4/24 Trial Tr. at 165:24 to 166:14.)

- American Casting and Manufacturing Metal Cup Seals With Gorilla Glue: Dr. Johnston was able to simply unscrew these seals by hand after the Gorilla Glue stuck the whole assembly together. (See Johnston Test., 4/21 Trial Tr. at 188:21 to 195:22.) Dr. Johnston testified that since he is able to remove and put the original Cup Seals back in their original locations, neither Level 1 nor Level 2 protocols would detect his attack on the Cup Seals with Gorilla Glue, or any comparable attack. (Johnston Test., 4/24 Trial Tr. at 35:2-4.)

1181. Level 3: Even though a Level 3 protocol would detect Dr. Johnston's attack, such a protocol for this seal would be enormously expensive and complex. Inspectors would have to take microphotographs of the seals at installation, and compare them with new microphotographs taken during inspection to detect otherwise invisible marks left by an attacker. (Johnston Test., 4/24 Trial Tr. at 35:7-11.) Like the other Level 3 protocols, this is too costly and complex for New Jersey to implement. (Johnston Test., 4/24 Trial Tr. at 165:24 to 166:14.)

1182. Dr. Johnston found that in one instance the glue stuck the entire seal to the sheet metal of the DRE, turning it into a lock, rather than a seal. (Johnston Test., 4/21 Trial Tr. at 173:23 to 174:2.) Dr. Johnston was able to completely remove the seal with bolt cutters and replace it with an identical cup seal.

1183. Converting cup seals into locks using gorilla glue is very problematic. As mentioned earlier, tamper-indicating seals only work when their appearance and behavior are predictable. (Johnston Test., 4/21 Trial Tr. at 174:14-23.) In the case of Cup Seals that adhere to the DRE, inspectors trying to remove the devices are prone to causing unpredictable damage to the DRE likely to result in false

positives during inspections. (Johnston Test., 4/21 Trial Tr. at 176:20 to 177:9.) When this happens, in Dr. Johnston's expert opinion, inspectors come to expect false positives; as a result, they learn to ignore damaged seals. As a result, they ignore evidence of real attacks. (Johnston Test., 4/21 Trial Tr. at 205:20 to 206:22.)

- Plastic Strap Seals: Dr. Johnston picked open the Plastic Strap Seals [redacted] Johnston Test., 4/21 Trial Tr. at 140:21-25, 144:16 to 145:4; Johnston Test., 4/24 Trial Tr. at 56:13-21.) New Jersey currently has no use protocols in place for this seal, putting it at Level 1. (Johnston Test., 4/21 Trial Tr. at 80:9.)

1184. Level 1: Dr. Johnston concluded that without use protocols, an inspector would not detect his attack on the Plastic Strap Seals, or any comparable attack. (Johnston Test., 4/24 Trial Tr. at 32:25 to 33:20.)

1185. Level 2: A Level 2 protocol would, in Dr. Johnston's opinion, stand at best a 50% chance of detecting his attack. (Johnston Test., 4/24 Trial Tr. at 44:17-23.)

1186. Level 3: Although Level 3 protocol would detect his attack, (Johnston Test., 4/24 Trial Tr. at 44:24-25), again, it is almost impossible to implement such a thorough security analysis. (Johnston Test., 4/24 Trial Tr. at 165:24 to 166:14.)

K. Dr. Johnston Performed His Attacks as Demonstrations. but He is Not a Practiced Attacker; Therefore, the Court Should Not Take His Timings as Definitive

1187. The time that Dr. Johnston took to perform each attack does not represent the time that a real attacker would take. Dr. Johnston readily admits that he is not skilled with his hands. (Johnston Test., 4/22 Trial Tr. at 84:25 to 85:1.) His expertise is in devising attacks, not in practicing them to perfection. (Id.) Dr. Johnston

testified that an attacker with more agile hands would defeat New Jersey's proposed seals in a fraction of the time that it took him. (Johnston Test., 4/21 Trial Tr. at 144:3-6.) Beyond manual dexterity, however, no special qualifications are needed: Dr. Johnston testified that his Vulnerability Assessment Team has had artists practice attacks, because of their skilled hands. (Johnston Test., 4/22 Trial Tr. at 84:22-25.)

1188. Further, Dr. Johnston has not had as much practice attacking the proposed seals as a real attacker would. (Johnston Test., 4/21 Trial Tr. at 144:3-6.) For example, Dr. Johnston practiced his attack on the Brooks Red Adhesive Tape Seal only 13 times. (Johnston Test., 4/22 Trial Tr. at 63:2-3.) Dr. Johnston testified that a real attacker would practice an attack hundreds of times. (Johnston Test., 4/21 Trial Tr. at 144:3-6.)

1189. Indeed, according to Dr. Johnston, the Vulnerability Assessment Team at Argonne does not focus on practicing attacks to perfection. (Johnston Test., 4/22 Trial Tr. at 84:10 to 85:4.) Instead, Dr. Johnston's team practices each attack just enough to show that it is a concern, so as to leave time for analyzing a broader range of attacks. (Id.) Dr. Johnston reported that an attacker, without the same overhead costs and tight schedule as Argonne, could spend as much time as she needs to perfect an attack. (Johnston Expert Report, ¶ 53.)

1190. Again, Dr. Johnston testified that it is crucial to take every conceivable attack seriously, whether or not it has been demonstrated to perfection. (Johnston Test., 4/21 Trial Tr. at 53:21 to 55:4.) Dr. Johnston performed his attacks as a proof of concept, without the benefit of manual dexterity or hours of practice, (Johnston

Test., 4/21 Trial Tr. at 144:3-6), but was nonetheless able to defeat every seal proposed for New Jersey's DREs. (See generally Johnston Test., 4/23 and 4/24 Trial Tr.) A real attacker would be able to defeat the seals and install a fraudulent vote-stealing program even faster. (Id.)

L. Dr. Johnston Has Successfully Altered Election Results by Attacking the DRE Voter Panel, Circumventing the State's Proposed Seals Altogether

1191. Dr. Johnston testified that the easiest way to defeat a seal is to go around it. (Johnston Test., 4/22 Trial Tr. at 147:3-5; see also P-82, Addendum to Johnston Expert Report, ¶ 2.) New Jersey's DREs have no security features protecting the panel on which voters actually enter their votes, allowing an attacker to bypass all nine seals proposed by the State. (Addendum to Expert Report of Roger Johnston, Ph.D., Docket No. MER-L-2691-04, ¶ 29 (hereinafter "Addendum to Johnston Expert Report.")) The voter panel comprises twelve identical subpanels, with buttons for voters to cast their votes.

1192. The subpanels are available to purchase, or can be taken from an unsecured voting machine in the warehouse. (Johnston Expert Report, ¶ 149.) Dr. Johnston has devised three successful attacks on the voter panels, which are described in his Expert Reports. Dr. Johnston also made a proffer to the Court explaining that he was prepared to demonstrate the attacks on the record, and explaining some details of the attacks. (See Proffer of Roger Johnston, Ph.D. Pursuant to New Jersey Court Rule 1:7-3, Docket No. MER-L-2691-04 (hereinafter Johnston Proffer.))

1193. The most devastating attack on the voter panel is what Dr. Johnston terms the "On/Off Attack." (Johnston Expert Report, ¶ 149.)

- Dr. Johnston is able to install a remote-control device on a subpanel, controllable from two hundred feet away, even through walls. (Addendum to Johnston Expert Report, ¶¶ 30-31; see also Johnston Proffer, ¶ 5.)
- When the device is activated, it alters the subpanel circuitry so that all votes cast are directed to one candidate, without altering the behavior of the subpanel: a voter who pushes the button to vote for Candidate A will see a light indicating that her vote has been tallied for Candidate A, but the machine will record a vote for Candidate B. (Addendum to Johnston Expert Report, ¶ 30; see also Johnston Proffer, ¶ 3.)
- When the remote-control device is switched off, the subpanel operates correctly, recording all votes as cast. (Addendum to Johnston Expert Report, ¶ 30; see also Johnston Proffer, ¶ 3.)

1194. An attacker is able to activate the device during voting to steal votes, and then turn it off at the end of the day so that the subpanel behaves correctly under testing; all he has to do is press a button on a pocket-sized transmitter. (Addendum to Johnston Expert Report, ¶ 30; see also Johnston Proffer, ¶ 4.)

1195. The total cost of this attack was $55, using equipment commonly used by hobbyists. (Addendum to Johnston Expert Report, ¶ 31.) Dr. Johnston's expert opinion is that a high-school-age hobbyist could successfully effectuate the "On/Off Attack." (Id. ¶ 32; see also Johnston Proffer, ¶ 5.)

1196. Dr. Johnston was able to steal votes more simply by altering the wiring in the subpanels to swap votes. (Johnston Expert Report, ¶ 148; see also Johnston Proffer, ¶ 3.) The subpanel swap takes about twenty seconds, (Johnston Expert Report, ¶ 148), and in Dr. Johnston's opinion can be performed by a twelve-year-old child. (Addendum to Johnston Expert Report, ¶ 32.)

1197. A practiced attacker could even modify the subpanel circuitry while behind the voting booth curtain in one or two minutes. (Johnston Expert Report, ¶ 148.)

1198. Dr. Johnston was able to install fraudulent subpanels in a DRE that was switched on and in voting mode without any problem. Once the fraudulent subpanel is installed, an attacker can modify the removed subpanel and install it in a new machine. (Id.) That way, an attacker need only acquire one subpanel to attack a series of machines.

1199. The simplest attack of all on the voting panel is to replace the ballot sheet with a forgery that switches one or more columns, so that the column marked "Candidate A" actually records votes for Candidate B. (Johnston Expert Report, ¶ 139.) The result is that a district likely to vote for Candidate A actually goes to Candidate B. New Jersey publicizes the position of each candidate on the ballot sheet well in advance of the election. (Id. ¶ 140.) An attacker can easily roll up a counterfeit ballot sheet and smuggle it into the booth hidden in the leg of his pants. (Id. ¶ 139.) A second attacker can reinstall a normal ballot sheet at the end of the election to avoid detection. (Id.) This attack takes less than thirty seconds by removing a few normal screws; there are no security features in place to prevent the swap. (Id. ¶ 140.)

1200. Any of these voter panel attacks exploit Dr. Johnston's basic insight, that avoiding security seals is the best way to defeat them. (Johnston Test., 4/22 Trial Tr. at 147:3-5.) Given these design flaws in the DRE, seals cannot provide effective protection.

M. Implementing an Effective Security Program Based on New Jersey's Proposed Tamper-Indicating Seals Would Involve Great Time And Expense

1. The State's Proposed Seals Will Not Provide Effective Security Without Detailed Use Protocols, Which Will Be Time-Consuming and Expensive to Develop

1201. Dr. Johnston testified that developing an adequate seal use protocol will take at least several months per seal. (Johnston Test., 4/21 Trial Tr. at 79:18-24.)

1202. New Jersey has proposed six different kinds of seals for use in nine locations on its DREs. It will take at least six months, possibly up to eighteen months, to lay the basic groundwork necessary for such a program to be effective. (Id.)

1203. Dr. Johnston estimated that developing a seal use protocol would cost between $50,000 and $300,000 per seal, or between $300,000 and $1.8 million, at the outset, just to establish the basic protocols. (Johnston Test., 4/22 Trial Tr. at 144:3-9.)

N. In Order to Provide Effective Security, the State's Proposed Seals Would Require Detailed Inspections and Training, at Great Cost to the Taxpayers

1204. Dr. Johnston testified that conducting effective seal inspections would cost the state approximately an additional $492,000 per election, on top of the up to $1.8 million it will need to spend on developing basic seal use protocols. (Johnston Test., 4/22 Trial Tr. at 138:18 to 142:11.) He testified about the basis for this conclusion:

- Removing and inspecting the seals (including checking the serial numbers), removing the screws on the sheet metal covers, interior electronics inspection, reinstalling the sheet metal covers, reinstalling the seals, and recording the new seal serial numbers seals: **12 minutes**. (Johnston Expert Report, ¶ 97.)

- Inspecting each of the 12 (subpanel) printed circuit boards inside the voters panel to look for modifications and alien electronics: **13 minutes**. (Id. ¶ 98.)
- Inspecting top, sides, and bottom of each DRE for damage: **4 minutes**. (Id. ¶ 99.)
- Additional time needed for dealing with Gorilla Glued seals, installing Red Tape Seals, and cleaning up adhesives: **15 minutes**. (Addendum to Johnston Expert Report, ¶ 35.)
- Total: 44 minutes.

1205. At 44 minutes per DRE, 11,000 DREs would take roughly 8,000 person-hours to inspect.[33] Dr. Johnston estimated the hourly cost of seal inspectors at $50, a conservative estimate. (Johnston Expert Report, ¶ 102.)

1206. The hourly cost of inspections may well exceed $50. (Id.) Technicians at federal facilities typically cost between $80 and $200. (Id.) A higher hourly rate, of course, yields a higher estimate of the overall cost of inspections.

1207. It is also necessary to train inspectors regularly, further inflating the cost of seal-based security. Dr. Johnston testified that inspectors must receive approximately 12 hours of hands-on training per seal. (Johnston Test., 4/22 Trial Tr. at 133:4 to 134:1.) To remain effective, the training must be repeated annually. (Johnston Test., 4/24 Trial Tr. at 151:11-13.)

1208. With six kinds of seals in nine locations, New Jersey would have to devote at least seventy-two hours of training each year for every seal inspector on its payroll. Furthermore, since maintenance staff would have to navigate the proposed seals in order to access batteries and circuitry, they would also need to be trained to remove, inspect, and reinstall all nine seals. (Id. at 150:9-11.)

---

[33] This figure is based on Dr. Johnston's estimates in his original and supplemental Expert Reports.

O. Retroactively Adding Security Products to an Insecurely Designed System Does Not Work; in Such Instances, Dr. Johnston and His Team Recommend Exploring Different Security Approaches

1209. Even if New Jersey could afford to implement its seal program properly, its DREs would not be secure from tampering. The fact is that no amount of retrofitting can remedy the inherent security flaws in New Jersey's proposed seals program. Dr. Johnston's expert opinion is that retrofitting a poorly designed system is never successful. (Johnston Test., 4/22 Trial Tr. at 155:5-21.) For a system to be secure, it must be designed securely, not modified as an afterthought. (Id.) Such efforts are not only costly, but futile in terms of security. (Id.) For that reason, Dr. Johnston's Vulnerability Assessment Team does not hesitate to recommend replacing an insecure system with one that is designed from the ground up with security in mind. (Id.)

1210. Dr. Johnston testified that New Jersey's proposed security seals, even if properly implemented, cannot cure the engrained design flaws in New Jersey's DREs. (Johnston Test., 4/22 Trial Tr. at 155:5-21; Johnston Expert Report, ¶ 64.)

1211. The State never introduced a single witness with any expertise in physical security. The State had three months from the time Dr. Johnston filed his first report to the time he took the stand to call an expert in physical security to testify on its behalf,[34] but failed to do so. Dr. Johnston even recommended that the State consult a physical security expert in his report. (Johnston Expert Report, ¶ 77.)

---

[34] Dr. Johnston's first report is dated February 2009. (Johnston Expert Report at 35.) He first took the stand on April 21, 2009.

There is no testimony at all before this Court to refute Dr. Johnston. This expert conclusions remain uncontroverted.

XV. Testimony of Wayne Wolf

1212. Professor Wayne Wolf serves as Distinguished Chair of Embedded Computing Systems and Georgia Research Alliance Eminent Scholar at Georgia Institute of Technology. (Testimony of Wayne Wolf ("Wolf Test."), May 11, 2009 Trial Tr. at 5:9-20; Wolf Report, ¶ 1; P-117 Exhibit A (C.V. at 1-2.))

1213. Professor Wolf received his Bachelor's degree, Master's degree, and Ph.D. in Electrical Engineering from Stanford University. Following the receipt of his Ph.D. in 1984, Professor Wolf accepted a position as Professor at Princeton University and subsequently joined the faculty at the Georgia Institute of Technology in 2007. (Wolf Test., 5/11 Trial Tr. at 14-23.)

1214. Professor Wolf was the founding editor-in-chief of the journal for the Association for Computing Machinery ("ACM"), TRANSACTIONS ON EMBEDDED COMPUTER SYSTEMS. (Wolf Test., 5/11 Trial Tr. at 12-19.) He also served as editor-in-chief of the Institute of Electrical and Electronics Engineers ("IEEE") journal, TRANSACTIONS ON VSLI SYSTEMS. (Id.) Professor Wolf has authored four major textbooks, including texts on VSLI ("Very Large Scale Integration"), FPGA-based system design, and embedded computing. (Wolf Test., 5/11 Trial Tr. at 14:20 to 15:1.)

1215. Professor Wolf is the recipient of many distinguished awards for his work on computer systems, including the Frederick E. Terman Award from the American Society for Engineering Education. (Wolf Test., 5/11 Trial Tr. at 15:5-9.) He has been named as a Fellow of both the IEEE and the ACM. (Wolf Test., 5/11 Trial Tr. at 15:10-11.)

1216. Professor Wolf was certified as an expert in microprocessors, including embedded computing, logic design, and VLSI design. (Wolf Test., 5/11 Trial Tr. at 24:2-15.) Professor Wolf was also certified as an expert in embedded system security. (Id. at 24:14 to 26:16.)

1217. Professor Wolf performed his expert work on behalf of Plaintiffs pro bono.

A. Fake Z80 Microprocessors Can Be Easily Replicated at Minimal Cost

1218. The Z80 microprocessor used in the Advantage DRE voting machines was developed in the late 1970s. The technology is well-understood and easily replicated. (Id. at 27:1-10; Wolf Report, ¶ 53.)

1219. It is possible to create a "fake Z80" microprocessor that looks like the original Z80 manufactured by the Zilog Company, but which is modified to change election-related data on a DRE voting machine. (Wolf Test., 5/11 Trial Tr. at 27:18 to 28:6, 31:20 to 32:6; Wolf Report, ¶ 5.) The fake Z80s could be created easily and inexpensively by undergraduate-level computer science students. (Wolf Test., 5/11 Trial Tr. at 33:9-14; 34:21-24; Wolf Report ¶¶ 6, 18.) These fake Z80s could be introduced into voting machines and used to execute software that would subvert New Jersey elections. (Wolf Test., 5/11 Trial Tr. at 42:11-14, 43:9-12; Wolf Report, ¶ 6.)

1220. Professor Wolf evaluated the testimony of defense witnesses Ed Smith of Sequoia and Dr. Michael Shamos and found numerous incorrect statements in their testimony. (Wolf Test., 5/11 Trial Tr. at 28:9 to 29:20, 30:21 to 31:19, 43:1-17; Wolf Report, ¶¶ 7, 39-52.) Professor Wolf found that Dr. Shamos and Mr. Smith underestimate the threat posed by fake Z80s to the integrity of New Jersey's voting machines. (Wolf Test., 5/11 Trial Tr. at 28:9 to 29:20, 30:21 to 31:19,

43:1-7; Wolf Report, ¶ 7.) Professor Wolf testified that he and many of his colleagues in industry, government, and academia are very concerned about the threat posed by modified computers. (Wolf Report, ¶ 7.)

B. A Fake Z80 Microprocessor Can Be Designed in 56 Hours by a Junior-Year Undergraduate Using a $16 Part

1221. At least ten thousand computer technicians in the United States and many more worldwide have the logic design skills necessary to create a fake Z80 microprocessor. (Wolf Test., 5/11 Trial Tr. at 41:17-20, 51:14 to 52:4; Wolf Report, ¶ 18.) These logic design skills are taught in junior year undergraduate courses at many U.S. universities. (Wolf Test., 5/11 Trial Tr. at 33:9-14; Wolf Report, ¶ 19.) A potential attacker could hire one of thousands of people to design a fake Z80. (Wolf Test., 5/11 Trial Tr. at 41:17-20; Wolf Report, ¶ 16.) The people hired to do the work would not need to know the intended use of the device they were designing. (Wolf Report, ¶ 16.)

1222. Exemplar Z80 microprocessor designs are available freely on the Internet. (Wolf Test., at Trial Tr. 29:13-16; Wolf Report, ¶¶ 16, 53.) Only a small number of changes in logic design are needed to create a fake Z80 that would execute an attacker's code at the proper time. (Wolf Test., at Trial Tr. 29:17-20; Wolf Report, ¶ 22.) Using an Internet-available design as a starting point, and utilizing a Field Programmable Gate Array (FPGA) as a microprocessor, a computer technician with ordinary experience in logic design could create a fake Z80 in 56 hours. (Wolf Test., 5/11 Trial Tr. at 32:16 to 33:2; Wolf Report, ¶ 23.) Advanced undergraduate students could complete the design in less time. (Wolf Test., 5/11 Trial Tr. at 34:4-8; Wolf Report, ¶ 23.)

1223. Professor identified the Xilinx XC3S200AN-4FTG256C as an example of an FPGA that could be effectively used as a fake Z80. (Wolf Test., 5/11 Trial Tr. at 34:14-20; Wolf Report, ¶ 25.) This Xilinx has more than enough logic and memory capacity to embody the fake Z80 and the modified software needed to corrupt election results. (Wolf Test., 5/11 Trial Tr. at 35:21 to 36:10; Wolf Report, ¶ 25.)

1224. The Xilinx XC3S200AN-4FTG256C is available for sale at $15.84 apiece from the Digikey website.[35] (Wolf Test., 5/11 Trial Tr. at 34:21-24, 38:10-20; Wolf Report, ¶ 26.) Quantity discounts would likely be available for attackers who wish to make bulk purchases. (Wolf Test., 5/11 Trial Tr. at 34:21-24; Wolf Report, ¶ 26.)

C. Several Incorrect Statements by Defense Witness Terwilliger Exaggerated the Cost and Misrepresented the Capacity of FPGAs

1225. Professor Wolf identified several incorrect statements by defense witness Paul Terwilliger. Each of these incorrect statements either exaggerated the cost of creating a FPGA fake Z80 or misrepresented the computing power of FPGAs. (Wolf Report, ¶ 10.)

1226. Mr. Terwilliger over-estimated the amount of memory needed to implement a fake Z80 that would subvert voting machine software. Mr. Terwilliger's over-estimate was based on the erroneous assumption that semiconductor memory is implemented in logic gates. In fact, semiconductor memory is implemented with

---

[35] www.digikey.com (quoted price as of April 5, 2009.)

specialized circuits. (Wolf Test., at Trial Tr. 35:8 to 36:7; Wolf Report, ¶ 11.) Much less memory is needed to implement a hostile, FPGA fake Z80 than Terwilliger stated. (Wolf Test., 5/11 Trial Tr. at 35:8 to 36:7; Wolf Report, ¶ 11.)

1227. Mr. Terwilliger dramatically under-estimated the amount of memory available in an FPGA. (Wolf Test., 5/11 Trial Tr. at 35:8 to 36:7; Wolf Report, ¶ 15.) Terwillger's testimony ignored the FPGA memory available via lookup tables, on-chip memory, and flash. (See Wolf Test., 5/11 Trial Tr. at 37:20 to 38:4; Wolf Report, ¶¶ 11, 13, 14.)

1228. Mr. Terwilliger incorrectly stated that an attacker, desiring to install a fake Z80, would have to store both modified and unmodified software in an FGPA. In fact, not all of the voting machine memory contents would have to be resident on the chip. (See Wolf Test., 5/11 Trial Tr. at 38:-9; Wolf Report, ¶¶ 11, 15.)

1229. Finally, Mr. Terwilliger exaggerated the cost of purchasing FPGAs for use as fake Z80s. (Wolf Test., 5/11 Trial Tr. at 38:10-20; Wolf Report, ¶15.) Many inexpensive FPGAs, including the Xilinx XC3S200AN-4FTG256C, have the memory to create a fake Z80. (Wolf Test., 5/11 Trial Tr. 34:14-20; Wolf Report, ¶ 26.) These FPGAs cost as little as $15.84 apiece. (Wolf Test., 5/11 Trial Tr. at 38:10-20; Wolf Report, ¶ 26.)

D. FPGA fake Z80s Can Be Cheaply and Effectively Re-Packaged to Look Like Real Z80 Microprocessors

1230. Once an attacker creates a fake Z80 using a FPGA, the chip can be cheaply and effectively re-packaged in a dual inline package (DIP). (Wolf Test., 5/11 Trial Tr. 39:1-20; Wolf Report, ¶ 27.) The original FPGA package can be removed through delidding. (Wolf Test., 5/11 Trial Tr. at 23:10-18, 46:19-24; Wolf

Report, ¶ 28.) The FPGA would then be re-packaged in either ceramic or plastic coating. (Wolf Report, ¶ 29.)

1231. Once a fake Z80 FPGA is re-packaged, it would be visually identical to a real Z80 microprocessor. (Wolf Test., 5/11 Trial Tr. at 44:15-45:9; Wolf Report, ¶ 28.)

1232. The cost of packaging an FPGA in plastic is $8 each. (Wolf Test., 5/11 Trial Tr. at 39:25-7; Wolf Report, ¶ 29.) The cost of packaging an FPGA in ceramic is $55 each. (Wolf Test., 5/11 Trial Tr. at 39:25-7; Wolf Report, ¶ 29.) Professor Wolf estimated the total FPGA fake Z80 production cost, including purchase of the FPGAs and ceramic re-packaging, to be $70 apiece. (Wolf Test., 5/11 Trial Tr. at 53:4-15; Wolf Report, ¶ 30.) Fake FPGAs could be produced with plastic repackaging for only $15 apiece. (Wolf Report, ¶ 30.)

E. Fake Z80s Can Also Cheaply and Effectively Made Using VLSI Technology

1233. Custom integrated circuits, known as VLSI, can be manufactured so that they are visually identical to real Z80 microprocessors. (Wolf Test., 5/11 Trial Tr. at 13:16-24, 20:8-14, 40:8-41:6; Wolf Report, ¶ 31.) Thousands of people in the United States, including senior-level undergraduate students and beginning graduate students, have the skills to create VLSI fake Z80s. (Wolf Test., 5/11 Trial Tr. at 33:9-16, 41:7-20, 51:14-52:4; Wolf Report, ¶ 32.) Professor Wolf, who has written VLSI textbooks that are translated into Chinese, testified that thousands of additional designers in foreign countries also have VLSI skills. (Wolf Test., 5/11 Trial Tr. at 41:21to 42:5, 51:14 to 52:4; Wolf Report, ¶ 34.)

1234. To create a VLSI fake Z80, an attacker would start with designs that are publicly available. (Wolf Test., 5/11 Trial Tr. at 34:21-35:5; Wolf Report, ¶ 35.) A reasonably skilled individual, using computer design tools, could complete a

VLSI fake Z80 in about 1000 hours, or about six months of forty-hour weeks. (Wolf Test., 5/11 Trial Tr. at 32:16 to 33:5; Wolf Report, ¶ 35.)

1235. The VLSI fake Z80 could fit the additional logic and memory required for the fake Z80 onto the same size chip as a real Z80. (Wolf Test., 5/11 Trial Tr. at 42:11-14; Wolf Report, ¶ 36.) This would be accomplished through a manufacturing process that simply uses smaller transistors than the real Z80, which is in fact a very old part. (Wolf Report, ¶¶ 36, 53.)

1236. An attacker could hire a semiconductor manufacturer to produce 500 VLSI fake Z80s, encased in ceramic packages, at a cost of $640 per chip. (Wolf Test., 5/11 Trial Tr. at 42:15-25; Wolf Report, ¶ 38.) Attackers could also produce higher volumes of chips at lower per-chip costs. (Wolf Test., 5/11 Trial Tr. at 42:15-25; Wolf Report, ¶ 38.) Attackers could potentially sell such fake Z80s to others who wish to subvert voting machines or other machines that use Z80 microprocessors. (Wolf Report, ¶ 38.)

F. Fake Z80 Microprocessors Are Extremely Difficult To Discover; The Defense's Proposed Detection Techniques Are Destructive And Unreliable

1237. Embedded Security Expert Wolf identified problems common to all of the defense's proposed methods for detection of fake Z80 microprocessors. (Wolf Test., 5/11 Trial Tr. at 23:4-18, 45:18 to 46:18, 46:19-25.) Most importantly, defendants' witnesses Smith and Terwilliger's discussions of both x-ray and delidding techniques assumed that all of the voting machines used the same Z80 microprocessors. (Wolf Report, ¶ 40.) Because New Jersey likely uses more than one type of Z80, x-ray and delidding techniques are likely to lead to a large

number of false positives that would make inspections much more expensive and time consuming. (Wolf Report, ¶ 40.)

1238. No evidence has been presented by Defendants that New Jersey keeps an inventory of which types of Z80 chips it uses in its DREs. (Wolf Report, ¶ 43.) To conduct such an inventory would require removing the motherboard of each DRE, opening up each DRE, and subjecting the DREs to a particular detection technique. This process would be very expensive and could damage the DREs. (Wolf Test., 5/11 Trial Tr. at 47:7-11; Wolf Report, ¶ 43.)

1239. Semiconductor manufacturers like Zilog, the Z80 manufacturer, modify parts for a number of reasons. They may, for example, change the layout of a chip to fix bugs or to improve their manufacturing yield. (Wolf Report, ¶ 41.) As part of this work, the manufacturer may modify the top layer of the chip. (Id.)

1240. Semiconductor manufacturers also may redesign a manufacturing process. Such redesigned chips may place a smaller, more powerful transistor on a chip with an identical package to a previous version. (Id. ¶ 42.)

1241. In cases of either a changed layout or a changed manufacturing process, detection techniques such as x-raying or delidding would indicate that the chip was a different size or had a different set of features, causing an inspector to erroneously flag a voting machine as having been tampered. These false positives would make the inspection process both more expensive and more time-consuming. (Id.)

1242. The AVC Advantage used in New Jersey elections has been manufactured over a period of decades. To the best of Plaintiffs' knowledge, New Jersey does not maintain records about the revisions or maintenance to the hardware of the

machines. In order for x-raying or delidding results to be cost-effective and reliable, a careful audit would have to be made of the motherboard revisions and the Z80 parts used to stuff those boards. (Id. ¶ 43.)

G. Visual Inspection is an Ineffective and Destructive Detection Technique

1243. Visual inspection would not discover any fake Z80 that had been put in a conforming dual inline package (DIP). (Wolf Test., 5/11 Trial Tr. at 45:2-16; Wolf Report, ¶ 45.) Visual inspection of the motherboard is not an effective countermeasure for either the repackaged FPGA fake Z80 or the VLSI fake Z80. (Wolf Test., 5/11 Trial Tr. at 45:10-16; Wolf Report, ¶ 45.)

1244. Visual inspection requires removing the circuit board and seals from the voting machine. The board would have to be replaced in the machine after visual inspection. This requires time and effort that increases the cost of the task. (Wolf Report, ¶ 44.)

H. X-Ray Analysis is a Destructive and Largely Ineffective Detection Technique

1245. X-ray analysis cannot determine any details of the circuitry of a chip. (Wolf Test., 5/11 Trial Tr. at 45:18-24.) It might not detect an FPGA that had been removed from its original package and repackaged. (Wolf Test., 5/11 Trial Tr. at 45:18 to 46:11; Wolf Report, ¶ 47.)

1246. X-ray analysis could not identify a VLSI fake Z80 that was the same physical size and shape as a real Z80. (Wolf Test., 5/11 Trial Tr. at 45:18 to 46:11; Wolf Report, ¶ 48.)

1247. X-ray analysis requires not only that the motherboard be removed, but that the board also be sent to a facility for x-raying. Removing the board incurs the risk of

damaging the board and its associated connectors. (See Wolf Test., 5/11 Trial Tr. at 46:12-16, 47:12-21; Wolf Report, ¶ 44.)

I. Delidding is a Destructive and Largely Ineffective Detection Technique

1248. Delidding would not reveal a VLSI fake Z80 that was the same size and shape as a real Z80, if the fake Z80 had a decoy top layer conforming to the real Z80's appearance. (Wolf Test., 5/11 Trial Tr. at 46:25 to 47:6; Wolf Report, ¶ 49.) Professor Wolf testified that an attacker could easily make a VLSI fake Z80 that would evade detection by delidding. (Wolf Test., 5/11 Trial Tr. at 31:20 to 32:6, 46:25 to 47:6, Wolf Report, ¶ 49.)

1249. Delidding can damage the motherboard of a voting machine. Delidding requires that a motherboard be removed and sent to a facility for removal of a chip and delidding of that chip. This process runs the risk of damaging the motherboard and its associated connectors. The chip itself would be de-soldered, removed from the motherboard, and destroyed by the delidding process. (Wolf Test., 5/11 Trial Tr. at 46:12-16, 47:12-21; Wolf Report, ¶¶ 44, 50.)

1250. The designer of a VLSI fake Z80 could make the chip identical to a real Z80 even after delidding by putting a fake top layer on the chip. This fake layer need only be a few microns thick in order to avoid detection. (Wolf Test., 5/11 Trial Tr. at 31:20 to 32:6; Wolf Report, ¶ 37.)

J. Radio Frequency Analysis is an Unproven, Expensive, and Destructive Detection Technique

1251. Radio frequency analysis as a means of detecting fake Z80s would require a great deal of experimentation and may not work. (Wolf Test., 5/11 Trial Tr. at 48:8-

11.) Radio frequency analysis is not currently used in the election context anywhere. (Smith Test., 3/19 Trial Tr. at 74:10-18.)

1252. Sequoia's proposed radio frequency analysis countermeasure, according to Professor Wolf, is highly speculative. (Wolf Report, ¶ 52.)

1253. Before a radio frequency analysis test could be done, signatures of the real Z80s and Z80s with fraudulent firmware would have to be found. (Id.) The tests to discover a reliable signature from a Z80 is a difficult process. (Wolf Test., 5/11 Trial Tr. at 49:11-24.) In order to find a fake Z80, an examiner must wait for the fake Z80 do something illicit that would then possibly create a distinguishable frequency. (Wolf Test., 5/11 Trial Tr. at 51:5-10.)

1254. All electronic devices are forced to limit the energy that they emit. (Wolf Test., 5/11 Trial Tr. at 48:19 to 49:9; Wolf Report, ¶ 53.) The AVC Advantage uses a Faraday Cage to regulate its emissions, but the cage could have the additional effect of altering the frequency of the Z80. (Id.)

1255. Additionally, a radio frequency analysis would have to be based on the assumption that all the Z80s are made the same way, which is not always correct. (Wolf Test., 5/11 Trial Tr. at 52:10-16.) Professor Wolf testified that it is possible to create a fake Z80 chip that released the same radio frequency as a real Z80. (Wolf Test., 5/11 Trial Tr. at 51:3-10.)

1256. The Federal Communications Commission regulations of electronic devices require that all voting machine manufacturers reduce their emissions. (Wolf Test., 5/11 Trial Tr. at 48:19 to 49:9; Wolf Report, ¶ 53.) Sequoia has enclosed the Z80 and the motherboard in a Faraday Casing. (Wolf Test., 5/11 Trial Tr. at

48:19 to 49:9; Wolf Report, ¶ 53.) In order to conduct a radio frequency analysis, New Jersey would have to open its DREs. (Wolf Test., 5/11 Trial Tr. at 48:8-11, 49:3-9; Wolf Report, ¶ 53.) In order to get a consistent signal, radio frequency antennas would then need to be placed within this metal casing. (Wolf Test., 5/11 Trial Tr. at 48:13-18; Wolf Report, ¶ 53.) The Faraday Casings themselves would have to be removed and reinserted to place the antennas in the AVC Advantage. (Wolf Test., 5/11 Trial Tr. at 48:19 to 49:5.) Seals may have to be removed and replaced in order to reach the metal casing. (Wolf Report, ¶ 53.) This takes an enormous amount of time and manpower for a test that is speculative at best. (Id.)