Jan 31 201

| | |
|---|---|
| MARK BANFIELD, et al.<br>Petitioners<br>v.<br>CAROL AICHELE,<br>Secretary of the Commonwealth,<br>Respondent | No. 422 M.D. 2006 |

**REPORT OF DOUGLAS W. JONES, PH.D. ON BEHALF OF PETITIONERS**

## Qualifications

1. My name is Douglas W. Jones. I am an Associate Professor at the University of Iowa, Department of Computer Science, where I have taught since 1980. I received my Ph.D. and MS degrees in Computer Science from the University of Illinois at Urbana Champaign, in 1980 and 1976, respectively, and a BS degree in Physics from Carnegie-Mellon University in 1973. My teaching has focused on computer architecture, operating systems and security.

2. My expertise in voting technology includes the following:

3. I served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems from 1994 to 2004, and chaired the board for 3 terms. This board examines all voting systems offered for sale in the state of Iowa to determine if they meet the requirements of Iowa law.

4. I was invited to testify before the United States Commission on Civil Rights on evaluating voting technology for their January 11, 2001 hearings in Tallahassee Florida. I was invited to testify before the House Science Committee on problems with voting systems and the applicable standards for their May 22, 2001 hearings. I was invited to testify at an April 17, 2002 hearing of the Federal Election Commission. At that hearing, I recommended changes to the draft voting system standards that were subsequently adopted as the 2002 FEC Voluntary Voting System Standards.

5. I have written a number of book chapters, including: Chapter 1 of *Secure Electronic Voting*, edited by Dimitris Gritzalis, published by Kluwer Academic Publishers in 2002; Perspectives on Electronic Voting, in *From Power Outages to Paper Trails: Experiences in Incorporating Technology into the Election Process*, edited by Michael Yard, published by the International Foundation for Electoral Systems (IFES) in 2007; On Optical Mark-Sense Scanning, a chapter of *Towards Trustworthy Elections: New Directions in Electronic Voting*, edited by David Chaum and published by Springer-Verlag in 2010; Kazakhstan: The Sailau E-Voting System, a chapter in *Direct Democracy: Progress and Pitfalls of Election Technology*, edited by Michael Yard and published by IFES in 2010.

6. My paper, *Auditing Elections*, was published in October, 2004 in the Communications of the Association for Computing Machinery.

7. I am one of the ten principal investigators in A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections (ACCURATE), a multi-institutional center awarded a 5-year research grant by the National Science Foundation starting in October 2005, renewed for one additional

year. I do not yet know the status of the successor grant.

8. I have served as an electronic voting expert for election observation and assessment missions run by the Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe in Kazakhstan (November 2005, August 2007) and Holland (November 2006).

9. In the summer of 2004, I consulted with Miami-Dade County to assess problems with their ES&S iVotronic touch-screen electronic voting system and to assess their pre-election testing of their touch screen and optical scan voting systems. As part of this consultation, I was able to examine the iVotronic and a substantial amount of accompanying documentation.

10. In December 2005, I was invited by the Arizona Senate Government Accountability and Reform Committee to investigate the Optech 4C absentee vote tabulation system being used in Maricopa County.

11. I served as an expert witness in the case of Conroy v. Dennis in Colorado in 2005, where I was asked to assess the voting system assessment process conducted by the State of Colorado. In this context, I was allowed to examine all documents submitted to Colorado by Diebold, ES&S, Hart and Sequoia in their most recent rounds of voting system certifications in that state.

12. My vita provides further documentation of my qualifications to testify as an expert witness in the field of voting technology, including a list of my publications and professional activities. My CV is available on my website http://www.cs.uiowa.edu/~jones/vita.html

13. I have not received nor do I expect to receive any compensation for my effort in preparing this report or for my services as an expert witness in this litigation.

**Documents Cited**

14. In this report, I am making specific reference to the following documents, but the opinions expressed below also rely on my review of the literature of computer security and voting system technology during the course of my career, including, among others, my prior reports in this case and the works cited there. My opinions are expressed to a reasonable degree of certainty and are based on the available information as of the date of this report. In the event that additional information becomes available, my opinions may change accordingly.

15. *Report of Respondent's Expert Michael I. Shamos*, Ph.D, J.D, July 11, 2011. Statements in this report are referenced here as Shamos ¶ xx, where xx is a paragraph number.

16. Auditing Elections, *Communications of the ACM, 47*, 10 (October 2004) 46-50, by Douglas W. Jones.

17. *Problems with Voting Systems and the Applicable Standards*, testimony before the House Science Committee, May 22, 2001.

18. *Parallel Testing: A menu of options*, prepared for the Miami-Dade County Elections Department, Aug. 12, 2004.

19. *Election Administration in the United States*, by Joseph Harris, published by the Brookings Institution, 1934; available on the web at: http://www.nist.gov/itl/vote/josephharrisrpt.cfm

20. *Electronic voting systems certified prior to the Help America Vote Act of 2002,* from the Pennsylvania Dep. of State, Jul. 27, 2005.

21. *Manual Audit Requirements*, from the Verified Voting Foundation, May 24, 2010.

22. Harri Hursti, *Diebold TSx Evaluation – Security Alert: May 11, 2006 Critical Security Issues*

*with the Diebold TSx*, released by Black Box Voting.

23. *Qualification Testing of the I-Mark Electronic Ballot Station*, Report No 45450-01, Wyle Laboratories, Huntsville Alabama, Sept. 10, 1996. This report is confidential; the only content disclosed here is material that was discussed in open meetings of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems.

24. *Report on the Pvote security review*, by Ka-Ping Yee, Nov. 14, 2007. Available from the Internet at http://pvote.org/docs/pvsr.pdf

25. *DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio*, Election Science Institute, Aug. 2006. Retrieved from the Internet Archive of http://bocc.cuyahogacounty.us/GSC/pdf/esi_cuyahoga_final.pdf accessible from http://wayback.archive.org/web/

26. The video transcript of the the certification of ES&S Unity Software, Feb. 17, 2005, COM078017.

27. This document does not contain any confidential, proprietary or trade-secret information.

**A permanent physical record** (25 P.S. §3031.1)

28. Shamos ¶ 45 notes that Pennsylvania law 25 P.S. §3031.1 only requires that electronic voting systems "provide for a permanent physical record of each vote cast." He concludes that this wording does not require that a machine actually produce, use or retain any such records. Shamos ¶ 46 states that the requirement that records actually have a degree of permanence comes from 42 U.S.C. §1974, which requires that records of Federal elections be retained for 22 months, and from section 6.5 of the Voluntary Voting System Guidelines, which rests on this statute. Reading 25 P.S. §3031.1 as a computer scientist accustomed to reading system specifications, I have difficulty imagining that it was intended merely to request a capability without requiring that that capability ever be used.

29. Shamos ¶ 46 states, that "it is not necessary to decide the question [of the permanence of electronic records] in this case. If all parties agree that paper records are permanent physical records, then since all six of the questioned DREs produce paper records, they satisfy the statute." Shamos ¶ 47-49 go on to discuss the relative permanence of paper and electronic records, pointing out that, while their degrees of permanence may differ, neither is permanent in any absolute sense. I do not dispute these facts, but they are not useful.

30. This line of argument leads me to wonder, would Dr. Shamos admit that any type of memory does not satisfy the permanence requirements of Pennsylvania law? DRAM, dynamic random-access memory, and SRAM, static random-access memory come to mind. Variations on these memory technologies hold the programs and data during processing on modern computerized systems. SRAM memory technologies forget when the power is removed. DRAM memory is even more transient, since they forget in a matter of seconds unless refreshed by the memory control system. Some older voting machines, notably the Optech line of precinct-count ballot scanners, use SRAM chips with battery backup in their removable memory cartridges, where more modern machines use flash memory chips.

31. This is relevant to our line of inquiry because all DRE voting systems store the voter's selections temporarily in one or the other of these categories of memory until the software in the voting system decides to store this data in some less temporary memory. In the case of the iVotronic, this data is copied to three internal flash memory chips, one copy on each chip. after the voter elects to cast the ballot. At the close of the polls, a copy of one of these flash memory

chips may be printed, uploaded by modem, or stored on a removable compact flash card. If there is any question about the integrity of the firmware in the voting system, each of these copying operations becomes suspect.

32. The copies in the flash memory on the machine will be erased the next time the machine is used in an election, typically well within the 22-month ballot retention period mandated by federal law. Therefore, the copy that is retained to satisfy the 22-month retention requirement set by 42 U.S.C. §1974 must be one of these secondary copies, or perhaps even something less, a copy of a secondary copy. Thus, this is, at best, a copy of what was in the internal flash memory, which is, in turn, a copy of what was in the DRE voting machine's primary memory.

33. When a copy is made by simple physical means such as a photograph onto photographic film or a photocopy made by an old-fashioned non-computerized photocopier, it is easy to presume that it is an authentic copy. When a copy is made by human transcription, we expect errors and if the authenticity of the copy is in doubt, we insist on careful comparison with the original. When a computer is used to make the copy, as in modern digital cameras and modern photocopiers, we trust them because the computer that is involved – inside the camera or inside the photocopier, has no knowledge of what it is copying and therefore could not easily make a copy that is both corrupt and difficult to recognize as such. When, however, the domain is limited, as with copying files of voting results, and when the agent making the copy is potentially suspect, as with the firmware inside a voting system, each copy is potentially suspect.

34. The printed ballot-image report or cast-vote record produced by the thermal printer on a DRE voting machine or by the full-page printer on an election management system is not simply a copy of the data that was retained in the memory of the voting system. The original data in the voting system is retained in a form that is resistant to any human interpretation, and the software or firmware used to print that data does considerable translation and interpretation in reducing the data to textual form for human consumption.

35. In his argument that the paper copy suffices as a permanent record, Dr. Shamos has not addressed this issue: In all of the machines in question, the copy in question may be printed after the polls close, either by the printer attached to the DRE voting machine (on thermal paper not unlike a cash register tape), or by a printer attached to the election management system (typically a laser printer, although mechanical dot-matrix printers remain in common use in election systems). Thus, at best, the paper record is printed after the fact, many hours after the first votes of the day were cast. It is quite possible that the printing may be done days later at the county elections office, and may never be done at all.

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

37. Let us accept for the moment the arguments that the paper copy is the permanent record, and that 25 P.S. §3031.1 does not require the creation of a permanent record, but only the ability to create it. Suppose that a county that has not printed this copy is asked to produce it, perhaps in the course of an election dispute. Does printing this copy in response to such a request make it the permanent record of the election? It seems to me a matter of common sense that the information from which the printout was created is serving as the primary official record in this

case, and that the acceptance of the paper copy as the permanent record implies that the primary record is not permanent. The truth of this does not seem to depend on whether the copy is made at the close of the polls or months later.

38. Shamos ¶ 50 contends that electronic memory is physical because the chips on which the data is stored are physical. I believe that we all will agree that the paper used for a paper record is physical, and so is the ink used to write on that paper, which can be observed with the naked eye. However, Shamos ¶ 50 argues that we should also grant that both the flash memory chips inside a computer are physical and so are the electrons used to record data within them, which cannot be observed without the aid of complex technology such as an electron microscope or a computer. By this argument, all memory is physical; even the reverberating echo in a concert hall is physical. This argument suggests, therefore, that the word *physical* in 25 P.S. §3031.1 places no constraint on the memory devices used. When I read 25 P.S. §3031.1 as a specification for a computer system, I interpret the word *physical* as being intended to constrain, in some way, the kind of record created. This suggests to me that the intended reading of the phrase "permanent physical record" should be a matter of common sense, where the word *physical* means something like *tangible*.

39. In fact, Shamos ¶ 123 appears to agree with me. He argues that the requirement in 25 P.S. §3031.7(11) that the voting machine be "constructed in a neat and workmanlike manner of durable material of good quality" does not apply to software because it "clearly refers to the physical manifestation of the voting machine" while "software is intangible" and "it is not 'of material' at all." In point of fact, software, as it exists in the memory of a computer, in flash memory, or in a disk file, is exactly as physical and exactly as tangible as any other data in that computer. To argue that there is a distinction in the physicality of the two seems extremely artificial.

40. It is my understanding that the physicality requirements of 25 P.S. §3031.1 were enacted in 1980. At that time, as I understand it, Pennsylvanians were voting on mechanical lever voting machines since 1929, according to Joseph Harris, page 247), and there were no approved electronic voting systems in use in the state. The most widely used electronic voting system at that time was the Votomatic punched-card ballot. According to the Pennsylvania Department of State, the CES Votomatic was approved on Jan. 30, 1981, and the Thornber Compact Vote, VOTPAC and ELPAC (also a punched-card system) were approved on Dec. 31, 1981. The AVM Voting Computer was approved on August 6, 1982. According to the Pennsylvania Department of State, this was the first DRE voting machine approved in Pennsylvania. I believe this was the first time the AVM Voting Computer was certified for use in any state. There is no reason to believe that the legislature did not intend there to be a tangible physical record comparable to that produced by the electronic voting systems then in use.

41. The record inside a mechanical lever voting machine is maintained on mechanical counters identical in operating principle to a mechanical automotive odometer. One such counter (one register) sits behind each lever on the face of the machine. When the curtain on the voting booth is opened, the register behind each candidate lever that was turned down is incremented. When the polls close, the record of the vote was transcribed to a paper form reporting the precinct vote totals. For most machines, this transcription was done by hand, from the registers exposed inside the back of the machine to the precinct-totals report form. Although there were proposals to equip these machines with mechanisms to create some kind of permanent record of each vote cast, as used around the country, these machines only recorded the running total of votes, and the paper records created at the precinct and used in the official canvass of the vote contained only the zeros report – a check that all counters were zero when the polls opened, and

the totals report, a record of the final total for each race.

42. Given this history, I suspect that the requirement for "a permanent physical record of each vote cast" in 25 P.S. §3031.1 was intended as a response to the lack of such a record in most mechanical lever voting machines, in contrast to punched cards, where the hole in the card is a tangible physical record of the vote, or paper ballots, whether machine-counted by an optical mark-sense reader or hand counted, where the voter's mark on the paper is a tangible physical record. The ballot-image reports or cast-vote records printed after the fact, perhaps long after the fact, are the product of complex computer software working from information retained from the time the voters cast their ballots. I cannot imagine that the permanent physical record requirement was drafted with an understanding that such a long chain of translation and copying would intervene between the voter's act of casting a ballot and the creation of a permanent record of that act. We have no way of knowing, at each step along this chain of translation and copying, that the information conveyed correctly records each vote cast.

**Materials and Workmanship**

43. Shamos ¶ 123 argues that 25 P.S. §3031.7(11) that the voting machine be "constructed in a neat and workmanlike manner of durable material of good quality" does not apply to software because it "clearly refers to the physical manifestation of the voting machine" while "software is intangible" and "it is not 'of material' at all." I disagree with this reading.

44. Computer software is clearly constructed by composing many component parts into a whole. Some of these components are purchased or found, others are created for the project at hand.

45. Neatness and workmanship do not apply only to tangible things, they apply to the intangible. Sentences may have sloppy grammar. If I as a programmer elect to use a particular off-the-shelf software component, and I do a bad job of evaluating it, I may easily be charged with failing to select "material of good quality" from which to build my software.

46. Given that the statute in question was written at a time when electronic voting was not used in Pennsylvania and when punched-card technology was the most widely used electronic voting technology, we can assume that the authors of the statute did not have complex expectations concerning the nature of computer software. Therefore, the question is, how did they intend that their statutes be extended in an era when entire voting systems are composed of software running on a hardware not greatly different from that used to construct common laptop computers. I believe that, under such circumstances, we must admit that the workmanship requirement be interpreted as applying to software. Otherwise the requirement would be largely meaningless in the context of DRE voting machines.

**A Statistical Recount** (25 P.S. §3031.17)

47. Shamos ¶ 51 states that the "statistical recount of a random sample of ballots" required by 25 P.S. §3031.17 "is not a forensic investigation seeking to determine whether election records were properly created, or even whether they have been tampered with." I agree that the requirement set by 25 P.S. §3031.17 does not address forensic investigations. Rather, 25 P.S. §3031.17 appears to me to be a post-election audit requirement patterned after California's "one percent manual tally" law, first enacted in 1965. I quote California Elections Code § 336.5 in full: " 'One percent manual tally' is the public process of manually tallying votes in 1 percent of the precincts, selected at random by the elections official, and in one precinct for each race not included in the randomly selected precincts. This procedure is conducted during the official canvass to verify the accuracy of the automated count." In adapting this idea to Pennsylvania, machine counting has been permitted and the number of ballots counted has been doubled from

one percent to two.

48. Post-election auditing of the sort required in California and Pennsylvania has become fairly common in recent years. In 2010, the Verified Voting Foundation released a document, *Manual Audit Requirements*, summarizing the legal requirements for such audits in 25 states and the District of Columbia. Pennsylvania's statistical recount requirement is interpreted as requiring such an audit in this survey, although a footnote asks how it is possible to conduct a meaningful audit using DRE voting machines as used in Pennsylvania. There are, of course, significant differences between the states, but generally, these audits involve some kind of independent count of the records of individual votes cast in randomly selected precincts and a comparison of the results with the official canvass figures for those precincts.

49. 25 P.S. §3031.17 is silent about its purpose, unlike the California statute quoted above. Shamos ¶ 51 concludes, without supporting argument, that "the purpose of a recount is to determine whether the original tabulation was performed accurately. It is a 're-count,' that is, a second count." I pointed out in my 2004 paper on Auditing Elections that recounts of original ballots accomplish significantly more than mere re-tabulation of the vote:

50. When the recount involves original ballots, it asks not only "was the arithmetic correct" but also "was the voter intent correctly interpreted." If the tabulating machine used to count the original ballots counted flyspecks as votes, or if it ignored marks that were obviously intended as votes, this will come out in a recount of original ballots.

51. In contrast, when the original ballots are not available for a recount, as with the DRE machines we are considering here, what is being done, as Dr. Shamos asserts, is mere retabulation. If a DRE voting machine somehow mislead voters about the ballot presentation or it failed to correctly record their votes, this will not be detected in a retabulation. That is why the Pennsylvania statute calling for a statistical recount requires the use of a method of "a type different" from that used in the original count.

52. Shamos ¶ 66 to 70 returns to this topic, distinguishing between the event logs and ballot image retention. I believe we agree that P.S. §3031.17 deals only with the latter and ignores the significant potential utility of the former. We agree that there are multiple types of audits, and that the event logs maintained by current voting systems are (perhaps regrettably) not relevant to the routine post-election auditing required by Pennsylvania law.

### Redundant Records

53. Shamos ¶ 113 argues that, with paper ballots, we have no redundant records, while DRE machines create redundant records. I agree entirely that redundancy is one of the keys to creating a trustworthy election system, but I disagree with his conclusion.

54. I agree that DRE machines retain redundant copies of information during the election. This has been a requirement of all versions of the Federal voting system standards since 1990. The iVotronic, for example, has three internal flash memory chips, and all critical data is stored in duplicate form in all three chips. At the close of the polls, additional copies of the data are created. Precinct totals may be printed on paper, and it is possible that ballot images or cast-vote records may be printed as well. The totals may be transmitted by modem. The data from one of the internal memories may be written to a removable compact flash card, and the totals may be saved in a PEB. Presuming that all of the copies are accurate and that they are actually subject to examination, the more copies are created and the more widely they are dispersed, the less likely it is that the data will be lost or that a corrupted version of the data will go unnoticed.

55. But, Dr. Shamos argues that there is nothing equivalent with paper ballots. In fact, so long as

precinct-count ballots are used (usually mark-sense technology these days), the ballots are scanned as they leave the voter's hands, and that scanning creates a redundant record. Furthermore, at the close of the polls, the data from typical precinct-count mark-sense scanners is dispersed in much the same way as data from DRE machines. Paper records may be printed at the precinct, electronic copies may be transmitted, and removable memory cartridges may be collected. Again, the more copies are made and the more widely they are dispersed, the better.

56. I want to note something critical here: In all but the newest of today's mark-sense ballot scanners, no actual image of the ballot is retained, only records of what votes the scanner identified on each ballot. Similarly, on today's DRE machines, references to a retained image of the voter's ballots do not refer to an actual visual image on the screen, but rather, a record of what votes the machine collected from that voter. With paper ballots, we do retain the paper original, and several modern scanners retain actual image scans of each ballot. With DRE voting, nothing resembling the original ballot, that is the ballot seen by the voter, is retained as a "record of each vote cast."

57. The situation is quite different with centrally counted paper ballots, including postal absentee ballots of all types, many provisional ballots, and the vast majority of punched card and mark-sense ballots from the 1960s through 1980s. These ballots exist in only a single copy as they are collected and transferred to the ballot tabulating center. Several people typically handle each ballot individually, and others handle the envelopes and ballot boxes. I agree with Dr. Shamos in his characterization of the security of such ballots.

**Alternatives to Hand Counting**

58. Shamos ¶ 120 argues that the requirement in 25 P.S. §3031.17 that the statistical audit use "manual, mechanical or electronic devices of a type different" than the one used in the first count allows a number of alternatives. He suggests that some systems provide for printouts that can be optically scanned by different equipment.

59. The principal problem with this is the definition of "of a type different." With punched-cards ballots, I can imagine satisfying this by doing the first count using a card-reader attached to a computer, and doing the statistical recount or audit using an electromechanical card sorter. Note that the card sorter is undeniably "of a type different" because it is not electronic and based on a technology that was mature a decade before the invention of the computer. Also note that, in 1980, punched cards were, by a wide margin, the most widely used electronic voting technology and the one most likely known to those who crafted this requirement.

60. In contrast, suppose I did my first count using DRE voting machines and election management software, for example, the Diebold TSx and GEMS. Suppose, in addition, that I printed the results on paper, as Shamos ¶ 120 suggests, and then scanned the paper to perform the recount, a feature of the TSx. Unfortunately, the only software I am aware of that can read and process this information is provided by the same vendor.

61. Alternatively, suppose we accept the electronic records produced by the voting system as being the permanent record, and we attempt to satisfy the statistical recount requirement with a hand count. In this case, the actual mechanism of the recount involves both the computer printing or displaying the cast-vote records or ballot images and hand counting of the votes indicated by the computer. It is entirely fair to ask whether this process is in fact "of a type different," since the printing or displaying of the votes to be counted was done by the same voting system that produced the initial count.

62. The question we must answer is, how much difference is required by the phrase "of a type

different." As a computer system designer attempting to infer the intent of a system specification written like this, I would attempt to infer the answer by asking what kind of differences offer any advantage, since this requirement must have been intended to accomplish some useful goal. Certainly, cosmetic differences would serve no useful purpose. Running the same software on a desktop PC for the first count, and on a TSx for the second is an example of such a cosmetic difference – because it is the same software that is doing the counting. If the counting software is the same but for one count, we directly process the data, while for the other, we write it out as bar codes and then read it back in before processing it with the same software, we have still failed to accomplish any useful purpose.

63. Shamos ¶ 120 also suggests that we could satisfy the "of a type different" requirement if "the removable electronic media that contain the ballot images can be inserted into a different type of machine, read and tabulated separately." This might have some merit if "a different type of machine" implied that the counting and tabulating software was different, but we can only be certain that it is different if it was independently developed. If significant parts of the software are the same, then, as I argued above, the difference becomes a mater of cosmetics. The package that contains the software is different, but it is still the same software.

64. If the intent of the "of a type different" requirement is to increase public confidence in the integrity of the tabulation, then the difference must be apparent to the public, particularly to those who are suspicious of the integrity of the result. Differences that are apparent only to a privileged observer with court ordered access to the source code under strong nondisclosure constraints do not suffice for this purpose. The difference must be apparent to the public, and the difference must be sufficient to convince the public that no potentially corrupt component included in the first count was also used in the second.

65. I conclude that the appropriate reading of the "of a type different" requirement in 25 P.S. §3031.17 is that the statistical recount be conducted using mechanisms that are sufficiently different that they convince a skeptical observer of the correctness of the initial count. Dr. Shamos, in the video transcript of his oral remarks given as an introduction to the testing of the ES&S Unity Software on February 17, 2005, says something very similar about the standard to which voting machines should be held.

## The Adequacy of Federal Testing

66. Shamos ¶ 53 to 62 discusses the history of the current Federal system of voting system testing by independent testing laboratories (ITAs) more recently described as voting system testing laboratories (VSTLs). I am very familiar with this process as a former voting system examiner for the state of Iowa and as a current member of the Technical Guidelines Development Committee that oversees the development of the Voluntary Voting Systems Guidelines on which VSTL testing is based.

67. Shamos ¶ 53 makes it clear that Pennsylvania's electronic voting statute, originally enacted in 1980, has changed in "only one important respect". Shamos ¶ 60 and 61 documents this change, made in 2002 in response to the passage of the Federal Help America Vote Act (HAVA). The substantial change is the addition of the requirement 25 P.S. §3031.5 (a). This allows voting systems to be submitted to for state examination only if "the voting system has been examined and approved by a federally recognized independent testing authority *and* if it meets any voting system performance and test standards established by the Federal Government." Note the word and (I have italicized it). This is two independent clauses, one requiring examination by an ITA and the second requiring conformance to the Federal performance and test standards.

68. I disagree that 25 P.S. §3031.5 can be read as removing any responsibility from the state, as Shamos ¶ 62 suggests. "... the Secretary of the Commonwealth shall examine the electronic voting system and shall make and file in his office his report ... stating whether, in his opinion, the system so examined can be safely used by voters at elections as provided in this act ..." (25 P.S. §3031.5(b)). I agree with Dr. Shamos that the Federal standards and ITA or VSTL testing markedly simplify the work the states must do. That is why I worked to ensure that Iowa required ITA testing prior to certification in that state. It is irresponsible, however, for a state to rely on ITA or VSTL testing without assessing the adequacy of those tests and determining if any requirements have not, in fact, been tested.

69. I have encountered numerous cases where ITA testing has clearly been deficient. I know that Dr. Shamos is also aware of significant ITA failures. In fact, in one case, on May 5, 2006, Dr. Shamos told me (by telephone) significant details about one such vulnerability in the then Diebold TSx. The detail involved the ability to replace the firmware on the TSx silently, without leaving evidence that it had been done, a vulnerability discovered by Harri Hursti and now known widely as the Hursti II Attack. Given that the 2006 Pennsylvania primary was on May 16, there was no way to correct this problem before the election, so Dr. Shamos proposed short-term procedural defenses to mitigate (to some extent) the vulnerability in question.

70. Shamos ¶ 396 explicitly admits that he "believed the pre-2007 ITA system to have been dysfunctional, and I still believe that it was." All of the voting system certifications that are the subject of this case were produced by that flawed system.

**Can We Prove that a System is Secure?**

71. In general, the security of a system cannot be demonstrated by testing. Tests can prove that a system is insecure, but the failure to prove insecurity does not imply security, it only implies that the people conducting the test did not find any flaws that might have been present. Therefore, Shamos ¶ 61 statement that Pennsylvania "delegates the 'testing' function not to the Secretary but to an independent testing authority" (ITA) is largely irrelevant to any question about the adequacy of the evaluation of the security of the system.

72. In general, the security of a system cannot be demonstrated by a source-code review. Such a review can identify security flaws, but the failure to find such flaws does not imply security, it only implies that the reviewer did not find any flaws that might have been present. The source-code reviews conducted by the ITAs are not useless, but they have a proven track record of overlooking serious security flaws.

73. I first became aware of this weakness of the ITA process when I read the 1996 report on the I-Mark Systems Electronic Ballot Station by Wyle Labs (an ITA). I read this in the process of a voting system examination for the state of Iowa. This machine was later renamed the Global Accu-Touch, and then the AccuVote TS. It is the direct ancestor of the TSx used in Pennsylvania, and in my source code review, I observed many places where original code from this machine clearly survives to this day. In that report, it was stated that the software for this voting system was the best that they had ever examined, and that they were particularly impressed by the security, particularly the use of cryptography.

74. In fact the same ITA report strongly suggested that the system in question had a major security flaw, one I was able to confirm in discussion with representatives of Global Election Systems at the examination. I scolded them for the shortcoming, and Iowa did not approve the system. I was shocked to find that this flaw was still present five years later, when Diebold's source code for the Accuvote TS was discovered on an openly accessible Internet site. The failure was obvious: The cryptographic key used for security on all Global and Diebold machines was a

constant. This is comparable to having the physical key to the lock used on a voting machine identical on every machine, an error that, in fact, Diebold also made.

75. The source code I examined for this case revealed that key management in the Diebold machine remains amateurish.

76. The shortcomings of source code examination were clearly demonstrated by Ka-Ping Yee in 2007. Yee created an extraordinarily simple DRE voting system called Pvote. The source code for Pvote was under 500 lines of text. He deliberately inserted 3 bugs in the program, each of which had serious security consequences, and then sent the code out to 6 well-known security experts for review. None of them found all of the bugs, and one of the bugs was not found by any of them, even though the reviewers had been warned that some bugs had been deliberately inserted.

77. In sum, security must be designed into computer systems, and if we care about security in the products we buy, our only hope is a design review. I have seen no evidence of anything approaching a design review in any of the work done by the ITAs or by the Commonwealth of Pennsylvania.

**Cryptography**

78. Shamos ¶ 149 admits that "hard-coding cryptographic keys that are intended to remain secret is not a sound practice" but then asks that the plaintiffs "explain how a needed key value could be introduced into the software in any other practical way." First, I do not see that it is our obligation to teach elementary computer security to either the Commonwealth or to the voting system vendors. If the Commonwealth and vendors lack sufficient expertise to evaluate and design appropriate cryptographic mechanisms, they should hire staff with that expertise.

79. I interpret this request for explanation to be an admission that the Commonwealth is unaware of a "sound practice" for solving this problem.

80. In our source-code evaluations, we criticized the lack of appropriate cryptographic key management for both the keys used to protect election results and for the keys used to protect the firmware update process. I have already related the story of my discovery in the 1990s of this flaw in the ancestor of the TSx. The need for good key management in cryptographic systems has been well understood for decades.

81. Some definitions are necessary: *Encryption* is the process of transforming a message from its original or plaintext form into an inscrutable encoded message. *Decryption* is the process or transforming a message from the encoded form back to the original plaintext. For our purposes, the words *encrypt*, *encode* and *encipher* are synonyms, as are the words *decrypt*, *decode* and *decipher*.

82. One widely understood approach to key management involves what is known as public-key cryptography. This has been widely studied outside the national security establishment since the late 1970s. Public-key cryptography is based on the idea of cryptographic codes where the key used to encrypt the message is not the same key as that used to decrypt the message. This is analogous to designing a door lock where the key used to lock the door is not the same one as the key used to unlock it.

83. With public-key cryptography, one of the two keys can be published. If the decryption key is published while the encryption key is held as a closely guarded secret, anyone can decrypt messages, but only if they were encrypted by the holder of the encryption key. This allows those who receive the messages to know, with a great degree of certainty, that the message is

authentic.

84. One way a voting system could prevent installation of software updates from any source other than the approved vendor would be to hard-code the vendor's public key into the voting system so that it is impossible to install updates without knowledge of the vendor's secret encryption key. There are alternatives to this approach to software update, but I believe that the current draft federal voluntary voting system guidelines are currently moving toward this model for software update.

85. Shamos ¶ 377 asserts that we have conceded that "the problem [of software update security where hard-coded encryption keys are used] may be remediated by taking physical security steps." This was in response to a statement that "this ... places increased importance on the physical security of every Edge, including those not currently being used." It is crucial to understand that the physical security steps in question here apply to every computer – the Edge in this case – currently containing this vulnerability. As there are Edge voting systems in use in many states, it is necessary that all states using the Edge properly secure their systems; otherwise, someone could gain access to the update key and use it in Pennsylvania. In fact, it is my understanding that Edge systems have already become available on the surplus marked and private individuals have obtained them and begun reverse engineering efforts.

**Flaws in the Machines Approved in Pennsylvania**

86. Shamos ¶ 73 dismisses the claim that the machines approved for use in Pennsylvania are flawed, insisting that "A system that violates one or more of the mandatory requirements of the Election Code is perforce 'flawed.' One that does not is not 'flawed.' " I agree that this is the correct criterion to use in this case. I note, however, that as I pointed out above, ITA testing and conformance to the Federal voting system standards (now called guidelines) are separate independent clauses in 25 P.S. §3031.5 (a). ITA approval is not, therefore, sufficient to demonstrate a lack of flaws.

87. Dr. Shamos dismisses out of hand many of the shortcomings I pointed out in my source-code reviews. Shamos ¶ 132 suggests that "a simple change to the iVotronic firmware would eliminate the problem." Indeed, for all of the design and implementation errors Paul Cotton and I found in our source-code examinations, changing the firmware could eliminate the problem.

88. I find the assertion in Shamos ¶ 132 that "It would not even be necessary for the vendor to submit the modified system for Federal testing for it to be used in Pennsylvania," to be alarming. This implies that so long as the voting system vendor says "all we're doing is fixing bugs," nobody is required to examine their work. In general, there is a need to allow for some class of *de minimis* changes, but in my experience, claims that "this change to software merely involves bug fixes" are very dangerous.

89. In my May 22, 2001 testimony before the House Science Committee on *Problems with Voting Systems and the Applicable Standards*, I described the consequences of one *de minimis* change gone wrong: In examining a touch-screen voting machine made by Fidlar and Chambers in the late 1990s, I found that the graphics of the ballot display subtly disclosed the previous voter's selections to the next voter. The fault was a change that had been made to Microsoft Windows. The release notes from Microsoft indicated that the change contained only bug fixes and cosmetic upgrades, so the ITA permitted as a *de minimis* change to a commercial off-the-shelf component. It was one of the "cosmetic" changes made by Microsoft that led to the violation of the right of the voter to a secret ballot.

90. In 2003, there were allegations that Diebold was changing the firmware on their voting systems

in California without even informing the state. On Nov. 13. California Secretary of State Kevin Shelly ordered a statewide audit of the voting system firmware and software in use in that state. The ensuing investigation showed that uncertified software from many vendors was in widespread use in California.

91. Given the problems described above, I cannot see how Pennsylvania can permit vendors to make changes to voting system firmware merely by asserting that the changes are bug fixes, yet this is what Shamos ¶ 132 appears to be saying.

92. Shamos ¶ 133 suggests a procedural remediation to the possibility that a voter could use a PDA or similar device to emulate the PEB required by an iVotronic to enable casting a vote. I agree with half of his remediation: Voters should never be allowed to handle PEBs. The other half of his defense, however, requires that pollworkers notice the beeping sound made by the iVotronic when the PEB is used. I have looked at event logs recorded by iVotronics used in Allegheny County in a general election several years ago. I found that each machine can handle about one voter every 3 minutes. If a precinct is busy, with long lines and several machines in heavy use, I have a hard time believing that a few extra beeps would attract anyone's attention.

93. In fact, in suggesting mitigation measures in Shamos ¶ 132, Dr. Shamos does not dispute that the iVotronic PEB attack allows a person to tamper with an iVotronic. While 25 P. S. § 3031.7(12) might be read as permitting "acceptable ballot security procedures," I do not agree with Dr. Shamos' suggestion that such procedures may be freely substituted for mechanisms. There are other parts of 25 P. S. § 3031.7 that appear significantly less forgiving. "No electronic voting system shall … be approved ... unless it shall be established that such system, at the time of such examination or reexamination" that it "(8) precludes each voter from voting or having his vote tabulated more than once ..." The iVotronic PEB attack could be used by a voter to do anything that can be done with a PEB, including voting more than once. I do not see an escape clause here permitting polling place procedures to substitute for the mechanism.

94. Shamos ¶ 131 asserts that it "is not a requirement of any state Election Code or of any Federal standard" that election procedures be "obvious, easy to remember, and easy to do." This is true, but it dodges an important point: Procedures that are ineffective because they are difficult and likely to be performed sloppily or ineffectively are of no value. I have come to this realization only after repeatedly encountering election procedures that were not carried out. For many years, I believed that better pollworker training and better pollworker manuals would suffice to eliminate such problems. I still believe that this can help, but I also believe that we are asking too much of pollworkers with many of todays' voting systems, and that the substitution of procedural defenses for technically sound systems is a doomed strategy.

95. Shamos ¶ 135 suggests that the fact that an attack was not actually demonstrated allows us to ignore the potential. I have long been troubled by an ethical dilemma in this regard. Developing and demonstrating a virus attack on voting machines would clearly add force to my criticism of the security of these machines, but a convincing demonstration would require showing how the virus worked, not merely asserting its existence. Such a demonstration would create the very real risk that the virus would be released into the world, and I do not want to do that. I believe that the vast majority of the critics of voting system security have reached similar conclusions. As a result, we limit ourselves to pointing out the theoretical possibility that a virus could be released. Instead of demanding that real viruses be demonstrated, we must be content with demonstrations that the key security vulnerabilities required to permit construction of a virus are present.

96. I believe that the Hursti report adequately demonstrated that the prerequisite security flaws are

present in the Diebold TSx to allow the construction of a virus that could be transmitted without likelihood of detection from TSx to TSx by way of the memory cartridges used to configure the machine for elections and collect and consolidate the results of elections. The severity of this vulnerability was later confirmed by every followup on Hursti's report. To build and demonstrate such a virus would pose a grave risk to all users of the TSx because of the possibility of its accidental release.

97. Shamos ¶ 136 suggests that parallel testing would be a viable way to meet the requirements of 25 P.S. §3031.17. I do not agree. I see no reading of this statute that would permit it to be satisfied by counting test ballots cast in a parallel test instead of counting the ballots cast by actual voters in a real election.

98. Parallel testing is, however, a useful idea, and I have long recommended it as being better than not testing but not necessarily as good as a system of post-election audits that compare ballot documents created by the voter with the machine tabulation of those documents, as I believe 25 P.S. §3031.17 was, in all probability, intended to require.

99. Parallel testing is expensive. While several states have undertaken efforts that have been described as parallel tests, I am not aware of any state that has opted to conduct more than a pilot project. A parallel test offering a reasonable assurance that no more than one vote in 100 had been tampered with in a particular election would require testing on the order of 100 machines in that election.

100. Good parallel testing is difficult. A crook who knows that his voting system software will be subject to a parallel test can take many measures to detect testing and make the machine behave honestly whenever it suspects a test tested. I do not believe that California's parallel tests, held up as an example by Dr. Shamos, would be difficult to defeat. In my 2004 report, *Parallel Testing: A menu of options*, written for Miami-Dade County, I noted that the most effective parallel tests appear to be the most intrusive, as they take place in the polling place in the presence of voters, while parallel tests that are done elsewhere or at other times are less intrusive but also less likely to be effective.

Executed on July 31, 2011, in Iowa City, Iowa.

Douglas W, Jones, PhD