5364154

FREDRIC D. WOOCHER (SBN 96689)
MICHAEL J. STRUMWASSER (SBN58413)
GREGORY G. LUKE (SBN 225373)
AIMEE E. DUDOVITZ (SBN 203914)
STRUMWASSER & WOOCHER LLP
100 Wilshire Boulevard, Suite 1900
Santa Monica, California 90401
Telephone: (310) 576-1233
Facsimile: (310) 319-0156

Attorneys for Petitioners, Plaintiffs, and Contestants

FILED
ALAMEDA COUNTY
JAN 2 9 2007
CLERK OF THE SUPERIOR COURT
By ________ Deputy

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF ALAMEDA

AMERICANS FOR SAFE ACCESS; JAMES BLAIR; MICHAEL L. GOODBAR; and DONALD O. TOLBERT,

Petitioners, Plaintiffs and Contestants,

v.

COUNTY OF ALAMEDA; DAVID MACDONALD, in his official capacity as Registrar of Voters for the County of Alameda; and DOES 1 through 20, inclusive,

Respondents and Defendants.

Case No. RG 04-192053

DECLARATION OF DOUGLAS W. JONES IN SUPPORT OF MOTION FOR SUMMARY ADJUDICATION AND IN OPPOSITION TO RESPONDENTS' MOTION FOR SUMMARY JUDGEMENT AND APPLICATION FOR *IN CAMERA* REVIEW

Priority Election Law Matter (Cal. Elec. Code §§ 13314(a)(3) and 16100 *et seq.*

Date: February 21, 2007
Time: 8:30
Dept.: 31, Hon. Winifred Smith

BY FAX

DECLARATION OF DOUGLAS W. JONES

I, DOUGLAS W. JONES, hereby declare:

1. I am an Associate Professor in the Department of Computer Science at the University of Iowa. I hc ld a Ph.D. in Computer Science from the University of Illinois at Urbana Champaign and have over th rty years' professional and academic experience in the study and teaching of computer systems. As re lected by my *curriculum vitae*, which was attached as Exhibit A to the Declarations I previously su mitted in this case on March 8, 2005, May 18, 2005, and July 7, 2005, I have extensive experience in the study, design, review, and use of computer systems for voting in elections. I have taught gr iduate courses, lectured before academic, professional, and government conferences, and authored published materials on this topic, notably as a contributor to the 2002 book, *Secure Electronic Voting*. (S e also "Auditing Elections," Communications of the Association for Computing Machinery, 47, 10 (C ct. 2004) 44-50.)

2. I have offered testimony in court cases around the country regarding electronic voting security is ues and have provided comments, presentations, and testimony to numerous state and federal el ctions agencies, including the United States Elections Assistance Commission Technical Guidelines Development Committee, the National Institute of Standards and Technology, the United St tes Civil Rights Commission, the New York State Board of Elections, and the Arizona Senate G vernment Accountability and Reform Committee. I have submitted numerous papers and pr sentations to the country's leading computer science and voting security associations. A complete lis of my relevant publications, position papers, and testimony before federal and state agencies and ac idemic research bodies can be found at http://www.cs.uiowa.edu/~jones/voting/.

3. I have also testified before the United States House of Representatives Committee on Science and th Federal Election Commission during its review of the proposed 2002 standards for certification an l testing of electronic voting technology. As described more fully below, I have also served on the Io va Board of Examiners for Voting Machines and Electronic Voting Systems for ten years, during wl ich time I have had occasion to review and analyze most of the direct-recording electronic ("DRE") voting machine systems marketed in the United States. I submit the following declaration based upon

my personal knowledge and experience reviewing the security features of DRE systems, my review of the relevant sections of 2003 *DRE Technical Security Assessment* commissioned by the Ohio Secretary of State and prepared by Compuware Corporation, Inc. ("Ohio Report," pages 21-80, available online at the Ohio Secretary of State's website: <http://www.sos.state.oh.us/sos/have/files/compuware.pdf>), my review of the report entitled "Security Analysis of the Diebold Accuvote-TS Voting System" dated September 13, 2006 (the "Princeton Report" available from the Princeton Information Technolgy policy web site: <http://itpolicy.princeton.edu/voting/ts-paper.pdf>), my review of the report of the California Voting System Technology Assessment Advisory Board entitled "Security Analysis of the Diebold AccuBasic Interpreter" (the "VSTAAB report"), my review of the December 3, 2004, recount request letter submitted by Debby Goldsberry and the subsequent correspondence between her and the Registrar of Alameda County, and my review of Respondents' pleadings, deposition testimony, and discovery responses in this case. I have personal knowledge of the statements herein and, if called upon to do so could and would testify competently thereto.

4. I have served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems from 1994 to 2004 and I chaired the board from Fall 1999 to early 2003. This board, appointed by the Secretary of Sate, examines and approves all voting machines before they can be offered for sale to county governments. To ensure that the board was comprised of experts who possess a deep understanding of computers and of robust methods for testing computerized voting systems, the Secretary of State's office asked for volunteers to serve on the board from the faculty of Iowa's institutions of higher learning. I volunteered and was appointed. The board met on demand, whenever a manufacturer wished to offer a new voting machine or a new modification of an existing machine for sale in the state of Iowa; typically, this required us to meet from three to six times a year.

5. Based upon my expertise in the field and my service on the Iowa State Board of Examiners, I was asked to testify at the U.S. Civil Rights Commission hearing in Tallahassee, Florida, on January 11, 2001. My observations regarding the vulnerabilities of DRE voting technology have been quoted by the New York Times, Business Week, the Fort Lauderdale Sun Sentinel, the St. Louis Post-Dispatch,

Scientific American, the Chronicle of Higher Education and other publications, and I have been a gı est on NPR's *Science Friday* and several other radio programs.

6. In the wake of the 2000 general election, the Iowa Secretary of State convened a state election reform task force to examine Iowa's laws governing recounts specifically and elections generally, and as chair of the Iowa Board of Examiners, I was an active participant in this effort. As a general matter, it is necessary that laws governing the use of DRE voting technology take account of the vulnerabilities of those systems in the same manner that the law adapted to regulate the safe and secure use of mechanical voting machines in the past. In addition to service to the state of Iowa, I have also consulted with the ACLU (Illinois Chapter), Miami-Dade County, and the Brennan Center for Justice on issues related to the recount of votes cast on DRE systems.

7. The testing of electronic voting systems is evolving rapidly, with many states mandating that all systems undergo review by independent, third-party testing labs. But despite such testing, the Iowa Board of Examiners has uncovered numerous flaws in various DRE voting systems, both because of subtle differences in election laws from one state to another, and because we sometimes find areas that the testing lab missed or areas that are poorly covered by Federal Election Commission standards.

8. I have been publicly critical of the 1990 Federal Election Commission standards for some time, and because part of the Help America Vote Act of 2001 (passed in revised form in 2002) focuses on the regulation of voting technology, I was asked to testify before the House Science Committee on May 22, 2001, along with witnesses from MIT, Bryn Mawr College and the National Institute for Standards and Technology. As the Federal Election Commission came out with new draft standards in 2001, I became heavily involved in the updating and review of those standards, leading to my testimony before the Federal Election Commission on April 17, 2002.

Summary of Expert Opinion

9. The conclusions offered in my prior Declarations in this case, reproduced below for the Court's convenience have not changed: redundant data, audit logs, and chain-of-custody records are essential to any post-election recount of votes cast on a Diebold Accuvote-TS DRE system. Without examining such materials, one cannot form even a provisional opinion about the accuracy of vote tallies

generated during the initial vote-tabulation process that was used to form the basis of the certified election results.

10. In addition to the opinions previously stated, I am aware that Respondents in this case claim that a recount is limited under California law to a "retabulation" of ballots. I understand that Respondents claim that they perform such a "retabulation" when they generate a print-out of information stored on the PCMCIA flash-memory cards used in an election by inserting those cards into a few DRE touchscreen units arrayed in a recount room some weeks after an election. As a matter of elementary computer science and logic, however, it is not possible to meaningfully "retabulate" ballots on a Diebold Accuvote-TS DRE system without reference to other sources of information, such as chain-of-custody records, that prove that the data allegedly being "retabulated" during the recount are the same data that was tabulated in the first instance. That Respondents believe they can "retabulate" ballots by reprinting the results from PCMCIA cards without reference to such meta-data indicates that they do not possess an elementary understanding of the nature of electronically stored data.

11. The factual premises of Respondents' Application for *In Camera* Review and the Declaration of Dave MacDonald are not sound. There are a variety of audit logs generated by the Accuvote-TS and by GEMS. I have examined many such audit logs obtained from other jurisdictions, and I have examined Diebold's documentation for the GEMS and for the Ballot Station firmware that runs on the Accuvote-TS. None of the audit logs I have seen and none of those illustrated in Diebold's manuals disclosed VARIABLE NAMES, in the way that term is usually used, and nothing they disclosed appeared to be of any potential use to a potential hacker. If I interpret the term VARIABLE NAMES as usually defined – that is, as a reference to named variables within the voting system firmware or software, there would be no reason to include these in an audit log, and such names would only be of use to a hacker if the hacker had access to the source code for the voting system firmware; that very same source code reveals all of the variable names, rendering any release of names in the audit log harmless. If I interpret the term VARIABLE NAMES as a reference to names that are commonly modified from election to election, most of these are obvious – names of the races and propositions on the ballot; disclosure of such names reveals nothing interesting.

12. In the Respondents' response to INTERROGATORY #19, the similar incorrect statements are made, that the audit logs contain information that "would assist persons who wish to hack any future elections." I am aware of nothing in the audit logs that poses any such threat.

13. The Responents' response to INTERROGATORIES #17 and #18 says: "Respondents/Defendants did not copy, upload or transmit AUDIT LOG data nor REDUNDANT DATA" from the voting machines. This is a surprising violation of the assumptions clearly stated in Diebold's GEMS Election Administrator's Guide, where the procedures for post-election processing clearly describe printing the audit logs as a normal activity that is conducted before the election results are certified. The same assumption is clearly stated in the GEMS User's Guide. Thus, the county's failure to retain copies of the event logs from an election violates Diebold's assumptions about how the system will be used.

14. It has always been my understanding that the Federal requirement that all ballots be retained for 22 months after any election involving federal offices applied not only to the ballots themselves, but also to pollbooks and all other records of the conduct of an election. It is the case that the audit logs retained by electronic voting machines record information that was formerly retained on paper, such as information about spoiled ballots. As such, it has always seemed to me that to fail to retain the audit logs would be irresponsible, at the very best.

15. I have both sets reviewed Respondents' Combined Responses to Petitioners' Requests for Admission in this case. In those Responses, Respondents deny that anomalies in audit logs, logic and accuracy test results, or chain-of-custody records could reflect, or lead to the discovery of, errors in reported vote totals generated by the Diebold Accuvote-TS DRE system. (Respondents' Combined Response to Request for Admission, Responses ## 29, 30, and 31.) Respondents also deny that discrepancies between the redundant data stored in each touchscreen unit's resident memory and the results generated by the central tally server could reflect, or lead to the discovery of, errors in reported vote totals generated by the Diebold Accuvote-TS DRE system. (Respondents' Combined Response to Request for Admission, Response # 28.) These denials contradict the basic principles of computer voting system security. Audit logs are created so that, in the event of questions about a computer system, the audit logs can be examined to see what happened. The fact that I have seen no evidence

that Alameda County has ever examined these audit logs suggests that these logs are not being used for the purpose for which they were designed.

Expert Opinion

16. It is my understanding that the Diebold Accuvote-TS system in use in Alameda County, California, was purchased, tested, and certified for use in California under the (now superseded) 1990 Federal Election Commission standards. In my opinion, these outdated testing standards were, and are, inadequate to ensure that DRE voting systems are reliable and reasonably safe from fraud or system error.

17. If a voting technology does not preserve and protect the ballots cast by voters in a tangible, physical format, then the only source of information about the accuracy of vote totals from a particular election is the design of the system itself. Secure system design falls into broad categories: (a) the software code and hardware of the machines, which, in most United States jurisdictions, is typically reviewed by a regulatory body or independent laboratory responsible for testing and certifying the machines; and (b) the capacity of the machines, and of the elections official who employ them, to generate data before, during, and after elections to demonstrate that the system has functioned properly.

18. Votes stored in electronic format are inherently subject to manipulation or corruption in a manner that is virtually impossible to detect without special expertise, and specifically access to and understanding of the system design. Because of this, all vendors of DRE technology incorporate some form of layered security system design involving data-storage redundancy and system self-monitoring. In addition, virtually all DRE system designs expect that the elections officials and poll workers who use the technology will observe appropriate system security protocols to diminish the opportunity for hacking, error, or other types of data corruption. While these layered redundancy and security systems by no means replicate deterministic capacity for review and recounting available to systems that retain physical ballots, they can, if well-designed and rigorously followed, provide some measure of assurance that the DRE systems in question have functioned as designed.

19. In the absence of the actual physical ballots cast by voters, a public, post-election "recount" of votes cast on DRE systems is not possible, in any meaningful sense, without public review of both the

system's software code and hardware, coupled by a thorough review of all the data generated by the machines and their handlers indicating that the machines have functioned as designed, and have been kept inviolate, during the course of a given election. It is my understanding that California contracts with independent testing laboratories to conduct the review of any given voting system's software code and hardware. In my experience, such independent testing procedures do not adequately prevent vulnerabilities and errors in system design. It is also my understanding, however, that the lawsuit in aid of which I submit this declaration does not presently involve a challenge to the adequacy of California's independent testing procedures. Instead, the action challenges the denial of access to other election materials that are also relevant to a recount of elections run on DRE systems. Because there is no physical ballot preserved by the DRE system employed in Alameda County, the public must rely on circumstantial evidence that votes have been properly counted in any given election. Such circumstantial evidence must include all the data generated by the machines and their handlers indicating that the machines have functioned as designed, and have been kept inviolate, during the course of a given election, along with sufficient information about the software code and hardware to make this data meaningful. Sources of such evidence include the design of the system, all copies of cast-vote data stored on the system, all copies of the audit logs generated by the system, and the chain-of custody documents maintained by those who operate the system.

20. The Diebold Accuvote-TS DRE system formerly used in Alameda County did not preserve the actual ballot viewed and cast by the voters at the polls; instead, it is designed to transmute the voters' preferences into binary, electronic code, and to store that electronic cast-vote data in two separate data files on each machine. This data can, in theory, later be accurately re-constituted and re-arranged as a facsimile of the ballot viewed by voters. The only assurance that such facsimiles, or the summary data that can be aggregated from individual cast-vote data files, is accurate or reliable comes from the soundness of the system hardware and software, and from the audit logs generated by the machines themselves and the chain-of-custody records maintained by the elections officials and poll workers who use them, which together reflect that the system has functioned properly and has been kept secure. There is no way to assess the accuracy of electronically stored votes without such information.

21. It is my understanding that California does not require that DRE systems operate on open source code platforms. It is also my understanding that California does not require that vendors of DRE voting systems allow public review of their system hardware. Software code and hardware review are performed by the Secretary of State's Office in conjunction with an independent testing laboratory. Because the "platform" and basic design of DRE systems are kept secret in California, the only information available to voters to support post-election review of the accuracy and integrity of electronically-stored data is thus the data generated by the system and its users to monitor proper function of the machines and to prevent unauthorized access.

22. The Diebold Accuvote-TS DRE system formerly used in Alameda County is designed to create audit logs of all events related to the function of machines during the course of elections. Audit logs purport to record all human interaction or intervention with the machine as well as other system events such as power loss and the opening and closing of polls. The capacity to generate audit logs was mandated in the 1990 Federal Election System voting system standards, and it is a well documented design element of the all Diebold voting systems. Both the Federal standards ad Diebold's documentation clearly imply that the purpose of the audit logs is to allow for a post-election assessment of the accuracy and integrity of the electronically stored vote data.

23. The Diebold Accuvote-TS DRE system formerly used in Alameda County is designed to record identical copies of cast-vote data on memory resident in each voting machine and on a removable PCMCIA card that is removed from each machine at the close of polls and transported to a central or intermediate vote tabulation facility for uploading onto a vote tabulation server. This so-called "redundant memory" is required by the FEC/NASED 1990 voting system standards and a major design element of the Diebold system meant to provide information relevant to post-election assessment of the accuracy and integrity of electronically stored vote data. It is my understanding that Alameda County uses two methods for uploading data from the PCMCIA cards to the central server: (1) by direct upload at the central facility; and (2) via an Intranet link from remote, intermediate vote tabulation centers around the county.

24. The Diebold Accuvote-TS DRE system formerly used in Alameda County is designed to run "logic and accuracy" self-tests before and after elections in order to demonstrate that the software and

hardware are in proper condition. Records of these "logic and accuracy" tests are a major design element of the Diebold system to provide additional information relevant to post-election assessment of the accuracy and integrity of electronically stored vote data. While it is my opinion that these tests do not and cannot effectively detect or prevent all malicious code within a DRE system, I nonetheless believe that these tests can detect some problems and, therefore, that the results from these tests are information relevant to post-election assessment of the accuracy and integrity of electronically stored vote data.

25. Based upon my work on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, my review of publicly available information from Diebold, Inc., regarding the operation of their Accurvote-TS system, my review of the Princeton Report, and upon my review of the relevant sections of the Ohio Report, I believe that another major component of the security design for the proper use of the Diebold system are protocols for keeping all system components safe from unauthorized access. The proper functioning of certain hardware and software security design elements are partially predicated on the observance of such security protocols. For instance, elections officials should employ some form of numbered, plastic seal when locking the Diebold machines before and after elections, and should maintain a record of those numbered seals along with the names of the persons who applied and/or broke those seals at appropriate times. In my understanding, the primary, time-honored method for enabling the post-election assessment of the integrity of electronically stored data is the maintenance of such "chain-of-custody" and system access records by the elections officials who use the Diebold machines.

26. It is also my understanding that California law provides any voter the right to request a "recount" of votes in any given contest and to request in connection with that recount a review of all ballots and "any other relevant election material." I agree with the former California Secretary of State, however, that DRE machines do not presently provide for a meaningful recount of votes cast in an election in the absence of a paper ballot verified by the voter at the time he or she casts her ballot. Specifically, the DRE system formerly used in Alameda County fails to provide a meaningful recount because it does not preserve any ballot viewed and cast by a voter. Even in the absence of ballots, however, California law allows voters to review "any other relevant election material." Accordingly, even if a

voter is denied a meaningful recount, it appears that he or she may nonetheless request in connection with that recount review of other relevant election materials that may assist him or her in the post-election assessment of the accuracy and integrity of electronically stored vote data. Because DRE systems like the one used in Alameda County do not preserve the actual ballots viewed and cast by voters for a recount, it is absolutely necessary for elections officials to provide access to other relevant election materials in order to provide some form of post-election assessment of the accuracy and integrity of electronically stored vote data. In fact, even where paper ballots do exist, audit logs, pollbooks and other materials remain relevant, as these can demonstrate that ballots have been added or removed between the time of the first count and the recount.

27. I have reviewed the recount request letter submitted by Debby Goldsberry on December 3, 2004, in connection with the November 2, 2004, election, as well as the subsequent correspondence between her and the Alameda County Registrar. In that correspondence, Ms. Goldsberry requested review of the type of information I have discussed in the preceding paragraphs, i.e., audit logs, redundant data, logic and accuracy test results, and "chain-of-custody" information for all system components. The information requested in her recount request letter is not only relevant but absolutely essential to any meaningful post-election assessment of the accuracy and integrity of electronically stored vote data on the Diebold DRE system used in Alameda County.

28. The 2003 *DRE Technical Security Assessment* commissioned by the Ohio Secretary of State and prepared by Compuware Corporation, Inc., in the relevant portions addressing the Diebold Accuvote-TS DRE system, identifies a number of security vulnerabilities that render examination of the information requested by Ms. Goldsberry even more critical to the post-election assessment of the accuracy and integrity of electronically stored vote data. For instance, as of late 2003, supervisory access to the machines could be gained by unauthorized persons who are aware that "1111" was the standard PIN issued nationwide by Diebold; further, the key to the DES encryption scheme used for cast-vote data was hard-coded into the system, allowing unauthorized persons to decrypt and alter votes transported on the removable PCMCIA cards. Most critically, the Ohio Report repeatedly criticizes the vulnerability of ballot definition files and cast-vote records any time the system is connected to an *unsecured* intranet or the Internet. It is my understanding that Alameda County

elections officials did upload cast vote data through an intranet system. Accordingly, it is critical that election officials limit access to the machines, and to the county intranet, only to authorized personnel an l record such access through "chain-of-custody" and system access records.

29. The Ohio Report puts strong emphasis on the Diebold system's capacity to generate and maintain records of logic and accuracy testing. Such tests do ensure that main processor and programmable memory of each DRE machine functions appropriately before and after elections. They are, accordingly, not only relevant but critical to any meaningful post-election assessment of the accuracy and integrity of electronically stored vote data.

30. On a similar vein, the Ohio Report presumes that the Diebold system would be used as designed to produce "zero tape" printouts before the opening of polls and "precinct tally printouts" at the close of polls. Such printouts provide a critical basis for checking that no unauthorized votes have been added to machine memory either before polls are open or before the final central tally has been generated. It is essential that "precinct tally printouts" be generated at each polling place upon the close of polls t provide a point of comparison against the vote tallies that are ultimately generated from the central tally facility. The opportunities for electronically stored vote date to be corrupted increase markedly when that data is transported, uploaded, or otherwise accessed. Accordingly, the printing of zero tape printouts and precinct tally printouts are not only relevant but critical to any meaningful post-election assessment of the accuracy and integrity of electronically stored vote data.

31. The Diebold system uses a proprietary program called GEMS, which uses data formats compatible with MS Access, for ballot definition and tallying. As noted in the Ohio Report, an unauthorized hacker could easily enter the MS Access database to modify data from an election. As documented in the Ohio Report, one can gain such access to the cast vote data without any special password. This potential vulnerability of the data underscores the relevance of "chain-of-custody" and system access records for the purpose of meaningful post-election assessment of the accuracy and integrity of electronically stored vote data.

32. The Ohio Report, along with other threat vulnerability studies that have been produced in the intervening years (e.g., the VSTAAB Report and the Princeton Report) uniformly confirm the importance of audit logs, redundant data, logic and accuracy test results, and the zero tape/precinct

tally printouts as part of the overall layered strategy for assuring the accuracy and integrity of electronically stored vote data on the Diebold DRE system. It is also apparent that such security and verification tools rely in large part on the observance of adequate custody and access protocols by elections officials and poll-workers. Accordingly, to form a meaningful opinion about whether a given election run on the Diebold system used in Alameda County has been tainted by fraud or error, a person requesting a recount must have access not only to the verification tools generated by the Diebold system itself, but also must be allowed to review "chain-of-custody" and system access records maintained by the elections officials. In my opinion, such materials are not only relevant but essential to meaningful post-election assessment of the accuracy and integrity of electronically stored vote data. Without review of such materials, and without the actual ballots cast by voters, neither a recount nor any meaningful post-election assessment of the accuracy of election data may be had with respect to the Diebold DRE system used in Alameda County.

33. In light of the fact that computer scientists such as Hari Hursti and the authors of the Princeton, VSTAAB, Ohio, and State of Maryland SAIC Reports have demonstrated the manifest vulnerabilities of the source code used in both Diebold DRE and optical scan ("OS") technology, chain-of-custody and audit logs remain highly relevant, if not essential, materials for the conduct of recounts even in counties such as Alameda, California that have abandoned their DRE systems and reverted to optical scan technology. The Accubasic Interpreter code used in both DRE and OS systems has been shown to be potentially vulnerable to non-obvious hacking that can alter the outcome of elections. The Sequoia equipment used in Alameda County has not been subject to intense security evaluation by outsiders, but my recent study of Sequoia's documentation (see pages 11 to 13 of <http://www.cs.uiowa.edu/~jones/voting/conroy_v_dennis_jones.pdf>) reveals that some of their materials are embarrassingly shallow, and they certainly do not give me any confidence that Sequoia's systems are any less prone to security problems than Diebold's systems. Regardless of the apparent weakness of Sequoia's system, as evidenced by their documentation, proper maintenance and retention of audit logs and similar information is as critical for the Sequoia system as for the Diebold system.

Meaningful "Retabulation" of Ballots Is Not Possible on Respondents' former DRE System

34. I am aware that Respondents in this case claim that a recount is limited under California law to a "r:tabulation" of ballots. I understand that Respondents claim that they perform such a "retabulation" when they generate a print-out of information stored on the PCMCIA flash-memory cards used in an election by inserting those cards into a few DRE touchscreen units arrayed in a recount room some weeks after an election. As a matter of elementary computer science and logic, however, it is not possible to meaningfully "retabulate" ballots on a Diebold Accuvote-TS DRE system without reference to other sources of information, such as chin-of-custody records, that prove that the data allegedly being "retabulated" during the recount are the same data that was tabulated in the first instance. That Respondents believe they can "retabulate" ballots by reprinting the results from PCMCIA cards without reference to such meta-data indicates that they do not possess an elementary understanding of the nature of electronically stored data.

35. Based on my review of the correspondence between Ms. Goldsberry and the Respondents before the recount, it is clear that Respondents offered to print out so-called ballot images by assembling the PCMCIA cards used in the election, loading them into a few touchscreen units arrayed in a recount room, and directing the touchscreen units to print out data from the cards. Respondents did not offer to assemble the touchscreen units used in the election and print out the data from the redundant memory in each unit's resident memory, as Ms. Goldsberry requested.

36. Re-printing information from a PCMCIA card is not, without reference to more information, a meaningful "retabulation" of anything, much less a "retabulation" of the ballots actually cast by voters at the polls on November 2, 2004. Before one can call any such exercise a "retabulation," one must first demonstrate that the data on the PCMCIA cards at the time of the printing of the ballot images is the same data that appeared on the cards at the time the cards were first loaded into the central tally server for the initial tabulation. As a matter of elementary computer science and logic, one cannot demonstrate this fact except by reference to circumstantial evidence such as chain-of-custody records indicating that the cards were stored safely and not accessed by unauthorized personnel in the intervening period. Respondents' assertion that they perform a "retabulation" of ballots without access to other sources of data has no basis in science and reflects a profound misunderstanding of the nature of electronically-stored data.

37. I also understand that Respondents claim that "the printed image of each voter's ballot from every touchscreen used in the election" was offered to Petitioners during the recount and that these printed images were "the only documents available" responsive to Petitioners' request for "redundant vote data stored on the DRE machines." (Decl. of Bradley Clark, ¶ 9. A.) The first claim is dangerously vague and the second is proved false by Respondents' own admission.

38. First, as explained above, one cannot meaningfully assert that one has generated a "printed image of each voter's ballot" without reference to external data sources such as chain-of-custody information. It is also clear that Respondents offered to generate these images from the data stored on the PCMCIA cards. Because the data from those cards had already been intergrating into the central tally server to generate the certified election results, the act of printing those images provides little to no information about the accuracy of the certified result. Said another way, if the data on the PCMCIA cards was manipulated after the cards were removed from the touchscreen units, both the certified results and the printed image would reflect corrupt data. By contrast, comparison of the certified results to the redundant data stored on each touchscreen unit's resident memory would offer some information about the accuracy of the results generated by the central tally server.

39. Second, as Respondents' themselves admit, however, "REDUNDANT DATA of votes cast in the November 2, 2004, election remained stored in the TOUCHSCREEN UNIT RESIDENT MEMORY of each TOUCHSCREEN UNIT until at least January 7, 2005", the date the recount at issue in this case was declared complete. (Respondents' Combined Response to Request for Admission # 24.) Accordingly, the contention in paragraph 9 of Mr. Clark's Declaration that nothing other than images printed from the PCMCIA cards, is quite obviously false. It is precisely the redundant data stored in each touchscreen unit that Petitioners sought to review in this case. Though available, Respondents did not provide or offer to provide it.

<u>Respondents' Factual Claims in Support of its Application for *In Camera* Review are Incorrect</u>

40. I have reviewed Respondents' Application for *In Camera* Review and the accompanying Declaration of Dave MaDonald. The factual premises of Respondents' Application for *In Camera* Review and the Declaration of Dave MacDonald are not sound. There are a variety of audit logs generated by the Accuvote-TS and by GEMS. I have examined many such audit logs obtained from

other jurisdictions, and I have examined Diebold's documentation for the GEMS and for the Ballot Station firmware that runs on the Accuvote-TS. None of the audit logs I have seen and none of those illustrated in Diebold's manuals disclosed VARIABLE NAMES, in the way that term is usually used, and nothing they disclosed appeared to be of any potential use to a potential hacker. If I interpret the term VARIABLE NAMES as usually defined – that is, as a reference to named variables within the voting system firmware or software, there would be no reason to include these in an audit log, and such names would only be of use to a hacker if the hacker had access to the source code for the voting system firmware; that very same source code reveals all of the variable names, rendering any release of names in the audit log harmless. If I interpret the term VARIABLE NAMES as a reference to names that are commonly modified from election to election, most of these are obvious – names of the races and propositions on the ballot; disclosure of such names reveals nothing interesting. Respondents' stated reasons for *in camera* review of audit logs do not bear up under scrutiny.

41. In the Respondents' response to INTERROGATORY #19, the similar incorrect statements are made, that the audit logs contain information that "would assist persons who wish to hack any future elections." I am aware of nothing in the audit logs that poses any such threat.

42. The Responents' response to INTERROGATORIES #17 and #18 says: "Respondents/Defendants did not copy, upload or transmit AUDIT LOG data nor REDUNDANT DATA" from the voting machines. This is a surprising violation of the assumptions clearly stated in Diebold's GEMS Election Administrator's Guide, where the procedures for post-election processing clearly describe printing the audit logs as a normal activity that is conducted before the election results are certified. The same assumption is clearly stated in the GEMS User's Guide. Thus, the county's failure to retain copies of the event logs from an election violates Diebold's assumptions about how the system will be used.

43. It has always been my understanding that the Federal requirement that all ballots be retained for 22 months after any election involving federal offices applied not only to the ballots themselves, but also to pollbooks and all other records of the conduct of an election. It is the case that the audit logs retained by electronic voting machines record information that was formerly retained on paper, such as information about spoiled ballots. As such, it has always seemed to me that to fail to retain the audit logs would be irresponsible, at the very best.

44. I have reviewed both sets Respondents' Combined Responses to Petitioners' Requests for Admission in this case. In those Responses, Respondents deny that anomalies in audit logs, logic and accuracy test results, or chain-of-custody records could reflect, or lead to the discovery of, errors in reported vote totals generated by the Diebold Accuvote-TS DRE system. (Respondents' Combined Response to Request for Admission, Responses ## 29, 30, and 31.) Respondents also deny that discrepancies between the redundant data stored in each touchscreen unit's resident memory and the results generated by the central tally server could reflect, or lead to the discovery of, errors in reported vote totals generated by the Diebold Accuvote-TS DRE system. (Respondents' Combined Response to Request for Admission, Response # 28.) These denials contradict the basic principles of computer voting system security. Audit logs are created so that, in the event of questions about a computer system, the audit logs can be examined to see what happened. The fact that I have seen no evidence that Alameda County has ever examined these audit logs suggests that these logs are not being used for the purpose for which they were designed.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

Executed this 29th day of January, 2007, at Iowa City, Iowa.

Douglas W. Jones