Aug 10 2004

FREDRIC D. WOOCHER (SBN 96689)
MICHAEL J. STRUMWASSER (SBN58413)
GREGORY G. LUKE (SBN 225373)
BECKY L. MONROE (SBN 224409)
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 and Plaintiffs

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF RIVERSIDE

LINDA SOUBIROUS; GRACE SLOCUM; ALLEN E. HILL; RUSSELL HENSON; and VERIFIEDVOTING.ORG, INC., a non-profit Delaware corporation headquartered in California, Petitioners and Plaintiffs, v. COUNTY OF RIVERSIDE; MISCHELLE TOWNSEND, in her official capacity as Registrar Of Voters for the County of Riverside; and DOES 1 through 20, inclusive, Respondents and Defendants.	Case No. RIC 415443 DECLARATION OF DOUGLAS W. JONES

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 hold a Ph.D. in Computer Science from the University of Illinois at Urbana Champaign and have over thirty years' professional and academic experience in the study and teaching of computer systems. As reflected by my *curriculum vitae*, which is attached to this Declaration as Exhibit A, I have extensive experience in the study, design, review, and use of computer systems for voting in elections. I have taught graduate 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*. I have also testified before the United States House of Representatives Committee on Science and the Federal Election Commission during its review of the proposed 2002 standards for certification and testing of electronic voting technology. As described more fully below, I have also served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems for ten years, during which 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"), and my review of the April 2, 2004, recount request letter submitted by Petitioner Linda Soubirous and the subsequent correspondence between her attorneys and the Registrar of Riverside County. I have personal knowledge of the statements herein and, if called upon to do so, could and would testify competently thereto.

2. I have served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems since 1994 and I chaired of the board from Fall 1999 to early 2003. This board, appointed by the Secretary of State, must examine and approve all voting machines before they can be offered for sale to county governments. To ensure that the board would comprise 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 was appointed from among the volunteers. The board meets on demand, whenever a manufacturer

wishes to offer a new voting machine or a new modification of an existing machine for sale in the state of Iowa; typically, this means we meet from three to 6 times a year.

3. 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 hearings in Tallahassee, Florida on Jan. 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 guest on NPR's *Science Friday* and several other radio programs.

4. 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 have been 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.

5. 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.

6. 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 Testing. 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

Technology

Federal Election Commission on April 17, 2002.

7. It is my understanding that the Sequoia AVC Edge system in use in Riverside, California was purchased, tested, and certified for use in California under the prior 1990 Federal Election Commission standards. In my opinion, these outdated testing standards were, and are, wholly inadequate to ensure that DRE voting systems are reliable and reasonably safe from fraud or system error.

8. 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.

9. 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.

10. 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 Riverside 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 self-audit records generated by the system, and the security logs generated by the persons who operate the system.

11. The DRE system used in Riverside County does 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 various types of data, generated by the machines themselves and 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.

12. 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.

13. The Sequoia AVC Edge DRE system ("Edge") used in Riverside 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 is a major design element of the Edge system to provide information relevant to post-election assessment of the accuracy and integrity of electronically stored vote data.

14. The Sequoia AVC Edge DRE system used in Riverside 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 Edge 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 Riverside 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.

15. The Sequoia AVC Edge DRE system used in Riverside 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 Edge 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 vendor-designed tests do not and can not 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.

16. Based upon my work on the Iowa Board of Board of Examiners for Voting Machines and

Electronic Voting Systems, my review of publicly available information from Sequoia Voting Systems, Inc. regarding the operation of their AVC Edge system, 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 Edge 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 Edge 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 Edge machines.

17. 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 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 used in Riverside 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 Riverside 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.

18. I have reviewed the recount request letter submitted by Linda Soubirous on April 2, 2004, in connection with the March 2, 2004, Supervisorial district election. In that letter, Ms. Soubirous 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 Edge DRE system used in Riverside County.

19. 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 Sequoia AVC Edge DRE system, identifies a number of security vulnerabilities that render examination of the information requested by Ms. Soubirous even more critical to the post-election assessment of the accuracy and integrity of electronically stored vote data. For instance, supervisory access to the machines can be gained by pressing the Activate button on the back of the machines after polling has been closed; further, there is no password or confirmation entry during the poll closure process and supervisor functions are not password protected. Accordingly, it is critical that election officials limit access to the machines only to authorized personnel and record such access through "chain-of-custody" and system access records.

20. The Ohio Report puts strong emphasis on the Edge 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.

21. On a similar vein, the Ohio Report presumed that the Edge 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 print-outs 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 to provide a point of comparison against the vote tallies that are ultimately generated from the central tally facility. The opportunities for electronically stored vote data 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.

22. The Edge system relies upon an over-the-counter program, WinEDS, for the ballot definitions and vote tallying. WinEDS employs an MS SQL Server 2000 database which uses a common protocol for date sharing and transfer: ODBC ("Open Database Connectivity"). As noted in the Ohio Report, using MS Access, another over-the-counter component of Microsoft systems, a hacker would be able to connect to the election results database and 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. Because ballot definitions and cast vote data are not encrypted on this system – even on the PCMCIA cards used to transport the data – the modification of vote data would be relatively easy to accomplish. 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.

22. The Ohio Report confirms 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 Edge 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 Edge system used in Riverside 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 Edge 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 Edge DRE system used in Riverside County.

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

Executed this 10th day of August, 2004, at Iowa City, Iowa.

Douglas W. Jones