1 JOHN EICHHORST (No. 139598)
   Email: jeichhorst@howardrice.com
2 MICHAEL L. GALLO (No. 220552)
   Email: mgallo@howardrice.com
3 JASON S. TAKENOUCHI (No. 234835)
   Email: jtakenouchi@howardrice.com
4 D'LONRA C. ELLIS (No. 239623)
   Email:dellis@howardrice.com
5 HOWARD RICE NEMEROVSKI CANADY
        FALK & RABKIN
6 A Professional Corporation
   Three Embarcadero Center, 7th Floor
7 San Francisco, California 94111-4024
   Telephone: 415/434-1600
8 Facsimile: 415/217-5910

9 LOWELL FINLEY (No. 104414)
   Email: lfinley@wwc.com
10 LAW OFFICES OF LOWELL FINLEY
   1605 Solano Avenue
11 Berkeley, California 94707
   Telephone: 510/290-8823
12 Facsimile: 415/723-7141

13 Attorneys for Plaintiffs/Petitioners

14   SUPERIOR COURT OF THE STATE OF CALIFORNIA

15   CITY AND COUNTY OF SAN FRANCISCO

16

17 | JOSEPH HOLDER, PETER CANTISANI,   No. CPF 06-506171
   | DOLORES HUERTA, JUDY BERTELSEN,
18 | CHARLES L. KRUGMAN, DAVID   Action Filed: March 21, 2006
   | HAGUE GOGGIN, ALYCE E. FRETLAND,
19 | HELEN ACOSTA, MARY C. KENNEDY,   Action Remanded to this Court:
   | CHARLES FOX, MARTY KRASNEY,   July 17, 2006
20 | MITCH CLOGG, BEN P. VAN METER,
   | NANCY TILCOCK, CHARLES O.   DECLARATION OF DR. DOUGLAS W.
21 | LOWERY, JR., LILLIAN RITT,   JONES IN SUPPORT OF PETITION
   | HAROLD C. CASE, SUSAN J. CASE,   FOR WRIT OF MANDATE AND
22 | KENNETH MARTIN STEVENSON,   MOTION FOR PRELIMINARY
   | LARRY MARKS, HARRY JOHN RAPF,   INJUNCTION
23 | MERRILEE DAVIES, BERNICE M.
   | KANDARIAN, VICTORIA POST, and   Date: August , 2006
24 | VERONICA ELSEA, individuals,   Time: 9:30 a.m.
   | Dep't: 302
25 | Plaintiffs/Petitioners,   Judge: Hon. Ronald E. Quidachay
   |
26 | v.   Trial Date: None Set
   |
27 | (see following page)
   |
28 | BRUCE MCPHERSON, as California

Secretary of State; ELAINE GINNOLD, as Elections Official of Alameda County; CANDACE J. GRUBBS, as Elections Official of Butte County; VICTOR E. SALAZAR, as Elections Official of Fresno County; ANN BARNETT, as Elections Official of Kern County; THERESA NAGEL, as Elections Official of Lassen County; CONNY McCORMACK, as Elections Official of Los Angeles County; MARSHA WHARFF, as Elections Official of Mendocino County; MAXINE MADISON, as Elections Official of Modoc County; KATHLEEN WILLIAMS, as Elections Official of Plumas County; MIKEL HASS, as Elections Official of San Diego County; DEBBIE HENCH, as Elections Official of San Joaquin County; COLLEEN BAKER, as Elections Official of Siskiyou County; and DOES 1 through 50,

Defendants/Respondents.

HOWARD
RICE
NEMEROVSKI
CANADY
FALK
& RABKIN
A Professional Corporation

I, Douglas W. Jones, hereby declare:

1. Except as otherwise indicated, this declaration is based on my personal knowledge, and if called as a witness, I could and would testify competently to the matters contained in it.

2. For the reasons discussed below, it is my opinion that Diebold's AV-TSx voting system is not secure against tampering that could affect the outcome of elections. This opinion is based on my training and professional experience as a professor of computer science specializing in computer security; my review of a large body of current scholarly work on the subject of electronic voting system security and of technical specifications and publications of DRE system manufacturers; and other information gathered over the years at conferences, seminars, and workshops on electronic voting systems. Experts in computer security commonly rely on each of these sources of information, including those reports and investigations of other computer security analysts which are discussed in the paragraphs below.

3. 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.

4. My expertise in voting technology includes the following:

(a) 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.

(b) 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.

(c) 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.

(d) I was invited to testify at an April 17, 2002 hearing of the Federal Election

-1-

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.

(e) I wrote Chapter 1 of Secure Electronic Voting, edited by Dimitris Gritzalis and published by Kluwer Academic Publishers in 2002.

(f) My paper, Auditing Elections, was published in October, 2004 in the Communications of the Association for Computing Machinery.

(g) 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.

(h) In November 2005, I was invited to Kazakhstan by the Office for Democratic Institutions and Human Rights of the Organization for Security and Cooperation in Europe to help assess the Kazakh electronic voting system.

Voting Systems and Voting System Certification

5. Secure voting is extremely difficult, whether done using manual, mechanical or electronic means. While the algorithms involved are trivial, requiring nothing more than a sum, for each candidate or ballot position, of the number of votes, the distributed nature of the computation and the number of participants pose immense problems. Elections involve an appreciable fraction of the entire national population as participants, and the history of election fraud includes examples that were perpetrated by every class of participant, from voter to polling place election judge to election administrator to voting system maintenance technician.

6. Most of the new voting systems that have been purchased in the past 5 years were built and tested to the Federal Election Commission's 1990 standards, although some of these systems and parts of others are now certified to the newer 2002 standards. I have written at length about the shortcomings of these standards, for example, in my testimony before the House Science Committee on May 22, 2001, and before the Federal Election Commission, on April 17, 2002.

7. While many older voting systems do have severe defects, the rush to fund the

-2-

purchase of large numbers of new voting systems in the aftermath of passage of the Help America Vote Act of 2002 (HAVA) was a mistake. This mistake was compounded by the delay of over a year between the passage of the act and the appointment of members to the Election Assistance Commission (EAC), and the mistake has been further compounded by the failure of the Congress to allocate the promised funding for the standards and best-practices activities of the EAC.

8. Proponents of HAVA, at the time it was passed, wanted the new voting system standards promulgated by the EAC to be in place in time to have an effect on the voting systems purchased using HAVA funds. That did not happen. It takes several years for the industry to respond to new voting system standards, as is well illustrated by the fact that most of the voting systems purchased since the issue of the new 2002 voting system standards were certified to the older 1990 standards. The EAC did not issue its new "Voluntary Voting System Guidelines" (2005 VVSG) until December 13, 2005, nearly two years after HAVA called for the standards to be issued. The new EAC standards by their own terms do not go into effect until 2007. The 2005 VVSG will therefore have little if any impact on purchasing decisions being made now, under the legal pressure of the HAVA deadline for placement of at least one disability accessible voting system in each polling place nationwide for the 2006 elections.

9. All of today's voting systems are software based, with the exception of hand-counted paper ballots and mechanical lever voting systems. The correctness of this software is central to the trustworthiness of our election results, and because the current system of software certification is seriously flawed, the move to computerized election technology has simply replaced known evils with poorly understood systems without necessarily addressing the underlying problems. This is essentially the same thing we did a century ago when most of the nation began its move from paper ballots to mechanical lever voting systems.

10. Our current system of voting system certification illustrates a major failure in voting system transparency. As things stand right now, voting system testing under the FEC/NASED voting system standards (1990 and 2002) is an entirely closed process. The

HOWARD
RICE
NEMEROVSKI
CANADY
FALK
& RABKIN
A Professional Corporation

testing authorities are not obligated to disclose any report of their testing to the public other than a simple pass-fail judgment, while hundreds of pages of test results are sent back to the vendors.

11. There is an overwhelming public interest in the integrity of our election machinery, and this interest extends to all questions about the competence and thoroughness of the testing to which our voting systems are subjected. As things stand, the voting system vendors have been allowed to hide behind a myth of thorough and painstaking testing, telling not only the public but also state and county authorities that these tests prove the security of their systems when they do no such thing.

12. The central problem with voting system certification is that no individual or small group of individuals can or should be trusted. The potential gains from a corrupt election are immense and over the course of history, this has driven many individuals and corrupt organizations to undertake great efforts to gain control over the machinery of elections. Therefore, a credible system of software certification for voting systems must rely on open disclosure of all software that can possibly have an impact on the outcome of the election. We do not have such open disclosure now, because the voting system vendors treat their software as proprietary trade secrets.

The Difficult Problem of Software Version Verification

13. To have confidence in an electronic voting system, it is necessary to verify that only specific, tested and certified software is used in any part of the voting system, whether in the voting booth, at the tabulating center or elsewhere. It is necessary but not sufficient because, as discussed above, the certification process itself is seriously flawed. The problem is, how can an observer assure himself or herself that the software that is actually in use is indeed the very same software that has been approved for use?

14. For the computer I am using to write these comments, I can begin to answer this question by clicking on the "About this Mac" option on my screen, which helpfully informs me that I am running Mac OS X Version 10.3.9. This message tells me, with real certainty, that I am not running an authentic version of, say, Mac OS Version 10.3.4, because we can

-4-

define authentic versions of the operating systems as those versions that honestly report their identity. Unfortunately, the self-reported identity of a piece of software does nothing to assure an observer that this software is honest. Any software, including voting system software, could easily be programmed to report any false version number when queried.

15. In the case of my computer system, I trust the self-report of the system only because I personally installed the original version of the operating system on this machine, using media provided by the vendor, and because I trust the vendor's software update product to make secure connections to their web server to install operating system upgrades. Thus, a central element of my own personal trust here is that I personally had physical control of this computer system since it originally came out of the box.

16. The use of "software fingerprints" computed by some cryptographically secure hash function, as some security specialists have recommended, does nothing to change this fact. So long as the observer is limited to inspecting the self-declaration of identity of the system, there is no way for the observer to know whether that identity is declared honestly or not. The self-declaration that a piece of software has some particular MD5 hash can definitively tell you that the system is not the correct system, if the announced hash value is not the correct one, but it cannot tell you that the system is correct, since dishonest software could easily report a dishonest number.

17. Only if the observer can directly examine the memory of the computer and compare it with a reference memory image can the observer really know that what is in the computer and what is authorized to be there are the same. If we allow this comparison, however, we compromise the author's right to retain this software as a trade secret. In addition, if we are not very careful, the same memory access that allows inspection can also allow modification, thus elevating the election observer to the status of a security threat.

18. It may be possible to protect proprietary software from disclosure to observers if we allow the observer to run their own software on the voting system, where their software has read-only access to the system memory and a very narrow channel through which the software can announce the cryptographically secure hash code it has computed. This

-5-

requires that the observer trust the processor on the system to accurately run the hash-checking software, it requires that the firewalls protecting the system from the observer's software be secure against attacks by the observer's software, and it requires careful design of the choked-down channel by which the observer's software can report the hash code without disclosing the proprietary software itself.

19. It is important to emphasize that, to my knowledge, no such verification system is used in any voting system currently sold or used in the United States. The State of Nevada, however, uses a system of similar sophistication to verify that the software used in electronic gaming equipment is indeed the software that they have certified.

Chain of Custody Vulnerabilities of Electronic Voting Systems

20. All modern electronic voting systems pose problems that follow directly from the miniaturization of the technology. Where the automatically recorded record of precinct vote totals from a lever machine was recorded on a sheet of paper described as a "bedsheet" because it was so large, the automatic totals produced by a typical precinct-count direct recording electronic (DRE) or optical scan voting system are recorded on media such as compact flash cards or PCMCIA cards. The largest electronic media in common use today include devices such as the Election Systems & Software (ES&S) PEB—used in the iVotronic DRE—which is about 1×3×6 inches in size, or the similarly sized memory pack found in the Optech III Eagle precinct-count ballot scanner.

21. If we confine ourselves to precinct-count optical scan or hand count paper ballot systems, note how easy it is for an observer to determine that the ballot box dumped out for hand counting is the same ballot box that was used by voters. Similarly, note how easy it is for an observer to determine that the bedsheet removed from the back of an automatic recording lever voting machine is the same one that the election judges sign and witness for delivery to the county building. In each case, it is easy because the object being observed is large and difficult to conceal.

22. In contrast, when a memory device the size of a large postage stamp or a pack of cigarettes is involved, as is the case with current DRE voting systems, it is vulnerable to

JONES DECL. ISO PET. FOR WRIT OF MANDATE & MOT. FOR PRELIM. INJUNCTION

sleight of hand manipulation. As a result, unlike conventional ballot boxes, it is almost impossible for an observer to see that the memory card inserted in the envelope for transport to the county building is indeed the one that was pulled from the machine only seconds earlier. Even if the California Secretary of State were to enforce the extra security measures mandated by his conditional certification of the Diebold AV-TSx and AV-OS voting systems, the risk of substitution of a different memory card at the time of its removal from the voting machine for transport to the county building remains serious. In fact, the California Secretary of State rejected the following recommendation in a report by his own Voting Systems Technical Analysis and Advisory Board ("VSTAAB") entitled "Security Analysis of the Diebold AccuBasic Interpreter" (the "VSTAAB Report"):

> It would also help to load and seal the memory card into the AV-OS unit at the warehouse in advance of the election, ship it in this state, and when the election is over, have poll workers return the entire machine (with the memory card still sealed inside) to the county collection point, where election officials would check that the seal remains undisturbed and record the number on the seal before removing the memory card. This would ensure that the memory card is protected by a tamper-evident seal for the entire time that it is outside the control of county and would reduce the opportunities for someone to tamper with the memory card while it is in transit. We recognize that these heightened procedural protections are likely to be somewhat burdensome, but as a short-term protection (until the source code can be fixed) they may be appropriate.

A true and correct copy of the VSTAAB Report is attached hereto as Exhibit A.

23. Instead, I am informed that California poll workers remove the memory cards from all of the DRE voting machines slated for use in the state—Diebold, Sequoia, ES&S and Hart—and deposit them in a sealed envelope to be transported to the county building. I am unaware of any requirements imposed on this procedure that would defend against sleight of hand manipulation.

-7-

Threats to Voting System Security

24.   There is ample documentation at this point demonstrating that many voting systems on the market today suffer from serious flaws in their security. I have written about this at length; a good short summary of the situation is contained in my open letter to the election officials of the State of Iowa, a position statement presented to the Iowa State Association of Counties, Des Moines, Iowa, March 17, 2004, at the invitation of Iowa Secretary of State Chet Culver. This is on the web at: http://www.cs.uiowa.edu/~jones/voting/iowaletter.pdf. As stated in the open letter, the InfoSENTRY and Compuware reports for Ohio "cover systems made by Diebold, Election Systems and Software, Hart InterCivic, and Sequoia. These 4 vendors, between them, dominate the marketplace for voting technology in the United States, and the Ohio reports make it clear that, indeed, the FEC/NASED standards process has not ensured that voting systems meet any useful security standards."

25.   In addition, unfortunately, many of the assessments of voting system security have contained serious defects. These defects reflect badly on voting system vendors, the independent testing authorities, and on security professionals, suggesting that voting system security is a sufficiently specialized domain that many security experts have not correctly identified some of the fundamental security requirements of the voting domain. I have written about this in my article Misassessment of Security in Computer-Based Election Systems, in RSA Cryptobytes, RSA Laboratories Volume 7, No. 2, Fall 2004, excerpts of which follow as paragraphs 34 through 44, with updates to reflect events since the original manuscript of this material.

26.   Many people believe that elections are really trivial, and when an election is conducted in a small group by a show of hands, security is not an issue. Everyone present can observe the entire process and determine the result for themselves. Security becomes an issue when the number of participants grows to the point that the voters cannot all vote in the same room, and it becomes an issue when secret ballots are introduced in order to protect the rights of voters who oppose the powerful or hold unpopular opinions.

-8-

HOWARD RICE NEMEROVSKI CANADY FALK & RABKIN
A Professional Corporation

27. When elections are distributed between many locations, we must secure the conveyance of data between these locations, not so much because of the possibility of eavesdropping, but because we need to assure ourselves that the data is authentic. In fact, almost all of the data we are interested in conveying is public. The ballot layout is usually published weeks before the election and the totals from the precinct are usually posted in public when the polls close. The only actual secrets included with this data are authentication keys being distributed for later use.

28. Unfortunately, these elementary facts appear to be lost on many voting system developers, evaluators and customers. The following examples illustrate this.

Incorrect Use Of Cryptography Consistently Since 1996 In What Is Now The Diebold DRE.

29. In the summer of 1996, a subcontractor working for Wyle Laboratories of Huntsville, Alabama evaluated the software of the Electronic Ballot Station, an innovative new voting system made by I-Mark Systems of Omaha Nebraska. In the review of this software, the subcontractor reported that this was the best voting system software they had ever seen, and they were particularly impressed by its security and its use of DES. (This information is contained in the Qualification Testing of the I-Mark Electronic Ballot Station, Report number 45450-01, Wyle Laboratories, Huntsville AL, 1996, 336 pages. Because this report is proprietary, only content discussed in open meetings of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems is discussed here.)

30. This system was brought before the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, on which I sat, on November 6, 1997 by Global Election Systems of McKinney, Texas, which had renamed the system the AccuTouch EBS 100. At that examination, it quickly became apparent that the use of DES in this system was quite naive. The question that exposed this was simple: Given that DES is a symmetric key cypher, the security of the system depends crucially on how the key management and distribution problems are solved. So, how are they solved?

31. The answer from Global was disappointing but difficult to draw out: There was

-9-

HOWARD
RICE
NEMEROVSKI
CANADY
FALK
& RABKIN
A Professional Corporation

1 no key management or key distribution problem because there was only one key and it was
2 hard coded into every copy of the system.

3 32. I pointed this out to the vendor's representatives who were present at the
4 examination, and I assumed that this was a sufficient action on my part. It seemed
5 unnecessary to raise a public alarm or to call in the press. The meeting where I pointed this
6 problem out was a public meeting, although I don't recall more than one or two county
7 election officials being present as members of the public. The minutes of the meeting are a
8 public record, available to anyone. They described the security vulnerability as follows:
9 "Dr. Jones also expressed concern about data encryption standards used to guarantee the
10 integrity of the data on the machine. DES requires the use of electronic keys to lock and
11 unlock all critical data. Currently all machines use the same key."

12 33. As I recall the discussion that was reported so tersely in the minutes, I told Bob
13 Urosevich and Barry Herron, the Global representatives at the meeting, that embedding the
14 encryption keys in the source code might be acceptable in a prototype proof-of-concept
15 system, but that they needed to do better key management before the system went into
16 widespread public use. I told them that, so long as the encryption keys were in the source
17 code, they needed to guarantee that the source code would be tightly guarded, and they
18 needed to guarantee that no voting systems would ever be sent to the landfill or to surplus
19 sales outlets without first deleting all object code from them.

20 34. Unfortunately, this primitive security system remained in use in 2003, by which
21 time Diebold had purchased Global Election Systems. *See* T. Kohno, A. Stubblefield, A.
22 Rubin and D. Wallach, Analysis of an Electronic Voting System, IEEE Symposium on
23 Security and Privacy, Oakland CA, May 2004. In 2006, an independent expert analysis of
24 the Diebold source code has confirmed that the same cryptographic key is still hard coded
25 into the Diebold AccuVote-TSx DRE voting system (the successor to the AccuTouch EBS
26 100). *See* VSTAAB Report at 20-21.

27 35. Hard coding the encryption key into every system produced in a single year
28 would create a serious security vulnerability. Leaving the key unchanged for 10 years is an

-10-

invitation to tampering. Diebold's crude approach to encryption is tantamount to an automobile manufacturer equipping every car it produced between 1997 and 2006 with an electronic door lock system that is protected against unauthorized entry by a single secret electronic code. Anyone who discovers the code could gain access to every car the company had produced in that 10-year period.

36. Here, it is clear that the use of cryptography created only the illusion of security. Yet it was sufficient to fool the examiner for Wyle Labs into believing that the system was secure. The fact that the Independent Testing Authority that had examined the system had not seen the security problem I had identified was as alarming as the security problem itself.

37. In the years that followed, Global was acquired by Diebold, and the AccuTouch was repackaged and re-branded as the AccuVote TS. Bob Urosevitch rose to President of Diebold Election Systems, and the AccuVote TS was widely adopted for use in many states. I assumed that the security vulnerability that I had identified had been fixed. But in July 2003, computer scientists Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan S. Wallach released a report entitled Analysis of an Electronic Voting System. This report has become known as the Hopkins Report. As it turned out, Global had left their source code on a public FTP site, and when these researchers examined it, they confirmed that neither Diebold nor Global had seen fit to make any repairs to the security problem I had identified. The DES key was still a constant exposed in the source code.

38. One of the follow-ups to the Hopkins Report was an examination of the Diebold AccuVote TS by RABA Technologies commissioned by the State of Maryland. The RABA Trusted Agent Report was issued on January 20, 2004. In addition to confirming the presence of the flaws reported in the Hopkins Report, the RABA report also documented a new security vulnerability. On page 19 of the Trusted Agent Report, item 3 begins: Load a PCMCIA card with an update file. The PCMCIA card can be used to update the software on the AccuVote-TS terminal. This can be done by placing a PCMCIA card with an update file into the terminal and rebooting the terminal. The update file allows an attacker to overwrite any file on the system." General Recommendation 10, on page 24 of the report, directly
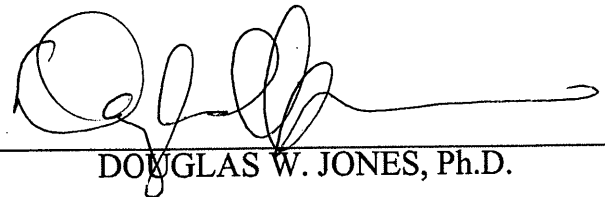
-11-

HOWARD
RICE
NEMEROVSKI
CANADY
FALK
& RABKIN
A Professional Corporation

addressed this vulnerability: "Do not allow software updates without authentication."

Old Diebold Security Flaws Left Uncorrected; New, Extremely
Serious Flaws Discovered

39. In an official Response to the Trusted Agent Report, issued on January 29, 2004, the State of Maryland assured the public that the recommendations in the RABA report were being taken seriously. This response itemized the state's response to the Immediate Recommendations of the Trusted Agent Report, but it was largely silent about the general recommendations. Nonetheless, it was reasonable to expect the vendor to implement the general recommendations, particularly those that were relatively straightforward, and it was reasonable to expect the State of Maryland to demand that Diebold do this.

40. A bit more than 2 years later, however, on May 11 of this year, Harri Hursti, in conjunction with Black Box Voting, issued a report entitled Diebold TSx Evaluation. This report clearly documents the fact that the security flaw documented in the RABA report is still present, and that, in fact, it is a much bigger problem than the RABA report had implied. There are actually three security flaws, technically differing from each other, but each allowing a devastating attack on the system from the PCMCIA card. A true and correct copy of Harri Hursti's Report is attached hereto as Exhibit B.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct and that this declaration was executed on August 7, 2006, at Iowa City, Iowa.

_____
DOUGLAS W. JONES, Ph.D.

-12-