

Douglas Jones, Ph.D.
201H MacLean Hall
University of Iowa
Iowa City, IA 52242-1419

September 5, 2006

Andrew C.S. Efaw
Wheeler Trigg Kennedy LLP
1801 California St., Ste. 3600
Denver, CO 80202

RE: Expert Report / Conroy et al v. Dennis

Dear Mr. Efaw:

This is my report in the Colorado Direct Recording Electronic ("DRE") case.

Qualifications

I am an associate professor of computer science at the University of Iowa. I have served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems for a decade ending in 2004 and was chairman of the board from late 1999 to early 2003. In that capacity, I routinely examined the technical data packages and independent testing authority reports for all voting systems submitted to the state of Iowa. I have testified on issues of voting technology before the United States Civil Rights Commission on January 11, 2001, before the House Science Committee on May 22, 2001, and before the Federal Election Commission on April 17, 2002. I consulted for Miami Dade County during the runup to the fall 2004 primary, and I consulted for the Arizona Senate Government Accountability and Reform Committee in December 2005, contributing to their investigation of the Arizona District 20 Republican Primary in 2004.

Along with co-investigators from Stanford University, the University of California at Berkeley, Rice University, and Johns Hopkins University, I am a principal investigator in NSF Grant CNS-052431 (ACCURATE), a 5-year competitive award starting in October 2005 establishing A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections. I served on the Brennan Center for Justice Task Force on Voting System Security, and contributed to their report *The Machinery of Democracy: Protecting Elections in an Electronic World* released this spring.

My CV, including a list of my publications and professional activities, is attached to this report as Appendix B. My vita provides further documentation of my qualifications to testify as an expert witness in the field of voting technology.

OPINIONS

My opinions are expressed to a reasonable degree of certainty and based on the available information as of the date of this report. In the event that additional information becomes available, my opinions may change accordingly. Document citations in what follows refer to documents by number from Appendix A.

Summary of Opinions

Based on my education, training, study, and experience in the field of voting technology, I conclude that the voting equipment certification process currently being used in Colorado is deeply flawed. The administrative rules adopted by the Secretary of State do not fulfill the requirements of the statute that authorized them, and the voting system examinations being performed under those rules are not effectively enforcing the rules. The weaknesses of the current system are most severe in the area of security standards and assessment. The state has demonstrated, in its evaluation of vendor documents, no understanding of which documents are and are not security critical. In its assessment of the Diebold and Sequoia voting systems, the state has overlooked significant security problems that ought to have been addressed prior to any decision to permit use of these machines in the state. Colorado statutes clearly require a much stronger process than the one I observed.

In the following sections, I will substantiate each of these general conclusions, explaining my reasoning and giving citations and occasional quotations from the documents I have examined. I have made every effort, in quoting from documents I have examined, to avoid any quotations that intrude on the proprietary interests of the vendors or the security interests of the state. It is my hope that this statement of opinion will be deemed to be part of the public record.

Opinion Regarding Flaws in the Certification Process

Earlier this year, a Colorado citizen, Al Kolwicz, filed a complaint with the Secretary of State regarding the Hart Intercivic E-Slate Voting System. In reading the Secretary of State's July 10 response to this complaint [1], I was struck by the lack of mention of any evaluation of the technical data package or independent testing laboratory reports submitted by the voting system vendor. At the top of page 10, we are simply assured that the submission is inspected for compliance with Election Rule 45.4.3 [2]. This rule states that "the voting system provider shall submit" a long list of documentation. It *does not require* that this documentation be evaluated. In the second paragraph on page 10, we are assured that "This office ... after review of the documentation submitted by Hart/InterCivic, deemed it was complete." Again, there is no indication that the documentation was actually read. John Gardner confirmed that indeed, much of this material is never read (page 137 line 5 to page 138 line 19 of [3] Volume I).

As a former voting system examiner for the state of Iowa, I find this incredible. In my experience, a voting system examination conducted without benefit of a review of the content of the technical data package and of the reports from the independent testing laboratories is unacceptable. I have found major security flaws in voting systems as a result of reviewing such documentation for the state of Iowa, including significant oversights by the independent testing laboratories and design weaknesses of the voting systems submitted to us.

This led me to read the statute authorizing the Secretary of State to adopt the Election Rules [4]. Colorado Revised Statute Section 1-5-616 paragraph (1) requires the development of rules "that establish minimum standards for ... voting systems regarding" among other things, (h) security and (i) telecommunications. Section 1-5-617 paragraph (2) requires that the Secretary of State's office *actually examine* the system.

Going back to the state's Election Rules [2], I conducted a review of Rule 45, which sets the state's voting system standards. Rules 37 and 38 are also relevant. I could find nothing in these rules that require actual evaluation, by the state, of information submitted by the vendors. Instead, many elements of these rules suggest careless drafting, oversights, and other problems.

John Gardner has testified that, to a significant extent, he was the author of Colorado's election rules, and that there was no significant oversight of the drafting process from the Secretary of

State (page 45 line 23 to page 51 line 18 of [3] Volume I). Gardner said that he also approves the County rules for use of these systems, again acknowledging that he does not read anything, but merely checks that documents exist (Page 150 line 9 to page 152 line 18 of [3] Volume I). By requiring documentation from the vendors that is never read, these rules effectively delegate large parts of voting system security to the vendors. As far as I can see, this does not set any minimum standard and therefore does not carry out Colorado Revised Statute Section 1-5-616 paragraph (1).

I found that definitions of significant terms sometimes contradicted the later use of those terms in the document. For example, Rule 45.1.2 defines an *audit log* as a paper record. Rule 45.1.3 defines a *ballot image log* as a “corresponding representation” of the votes cast. Corresponding to what? The terms *audit log* and *ballot image* are widely used with distinct meanings in the various voting system standards promulgated by the National Association of State Election Directors, the Federal Election Commission and the Election Assistance Commission. Rule 45.5.2.5.1 blurs the distinction by saying “except for the storage of vote images that shall be maintained in a random sequence, the audit records...” This appears to imply that the vote records are part of the audit records and not stored distinctly from them. I strongly suspect that this confusion results from conflating the long-established idea that voting systems maintain audit logs with the newer and quite distinct idea of a *voter verified paper audit trail*.

Similarly, Rule 45.1.5 limits its definition of a *communications device* to a device used to transmit tabulation data. Rule 45.5.2.7 defines *telecommunications* very broadly (and appropriately), but without reference to communications devices, even though the connection is obvious. This is evidence of sloppy drafting, at the very least.

Rule 45.1.6 is an eccentric definition of a *direct recording electronic* voting machine in two ways: It limits itself to mechanical and electro-optical interfaces (there are touch-screen input technologies that are neither). The second problem is potentially more serious: The rule lists secondary performance requirements such as storage of results “in a removable memory component and as printed copy.” As a result, a direct-recording electronic voting machine that does not have one of these characteristics is defined out of existence instead of being merely out of compliance with Colorado’s requirements. For example, the Diebold TSx, as used in Maryland Georgia and other states where the AccuView printer is not permitted, is not a direct-recording electronic voting machine under this rule.

Rule 45.2.1 makes it clear that Colorado approves entire systems, not components, and Rule 45.3.1 makes it clear that “any change made to individual components ... shall require recertification.” Later, however, Rule 45.5.2.2.4 discusses third-party hardware and software, and allows the vendor to document “a workaround for the end user to overcome” problems caused by such third-party components. This rule makes sense only if I assume that these third-party components were not fully integrated into the voting system at the time of state certification, and that end-users are expected to make changes without a requirement for recertification. Similarly, Rule 45.5.2.6.3 makes sense only if I assume that the vendor may recommend the use of security devices that were not part of the system as certified. Rule 45.5.2.7.6 is even more dangerous, since it clearly anticipates that election officials will be able to configure and install voting systems, and the word “configure”, as used in computer science, implies that the system as installed can be different from the system tested.

Rules 45.2.1 and 45.3.1 are also problematic. The central problem is one of drawing the border around the system that is approved as a unit and those parts that may be subject to local change. Power cords, printer paper and many other components must meet certain specifications, but a change of power cord from one purchased at Ace Hardware to one purchased at True Value does not threaten certification. I did not find any rules that allow a clear line to be drawn around the part of the system that requires certification and the parts where the county has some freedom to

reconfigure, select optional components, integrate third-party components into the system.

I read Rule 45.3.3 (b) as a promise by the Secretary of State to evaluate the documentation submitted by the voting system provider. The time limit of 16 days allows enough time for a thorough reading of a typical technical data package and is long enough to suggest that more than a cursory inventory of the submitted documents is required. Rules 45.4.3 and 45.5.2.6.1 require submission of massive piles of documents, but there are no apparent requirements against which these documents can be evaluated. In reading through the technical data packages provided by vendors, both in the past and in materials I have read for this case, I have frequently found documents that were obviously produced to fulfill such a vacuous requirement. These documents may be long and heavy, but they frequently say very little. I will discuss specific examples below, as I discuss the submissions from specific voting system vendors.

Some apparently objective requirements set by these rules are, on close scrutiny, quite soft. For example, rule 45.5.2.1.12 (a) requires that data exports that are “necessary for the SOS shall conform to XML format.” Unfortunately, XML is a huge family of related document formats, and the mere fact of data export in some XML format does not guarantee that the Secretary of State will have an easy time using that data. Similarly, the speed requirements set by Rule 45.5.2.2.2 (a) for “DRE/Touch Screen = 20 ballots per hour” say nothing about the type of ballot. Most direct-recording electronic voting machines can handle 20 ballots per hour for a single-issue bond referendum, but in my experience, few can handle ballots at this rate for a large general election ballot.

The permissive wording of Rule 45.5.2.3.10 is simply odd. It is not clear that it is possible to violate this rule. If the purpose of the rule is to explicitly inform the vendors that, unlike some states, Colorado does not constrain the use of rows or columns and does not constrain the segmentation of the ballot, why not just say so?

Rule 45.5.2.3.15 deals with “a control subsystem that consists of ... physical devices and software,” yet paragraph (b) “error detection” deals with “a detailed list and description of the error messages that will appear on the voting devices.” Paragraph (b) does not appear to relate to the control subsystem, nor is it an error detection requirement. Rather, it is a documentation requirement, on a par with Rules 45.4.3 and 45.5.2.6.2. As a result, there is no discussion of physical devices and software for error detection anywhere in this rule.

Rule 45.5.2.6.1, is a central security requirement, yet it is full of double and triple negatives that it is unworkable. Some sections appear to be wrong. Consider “at no time shall a system allow for unauthorized changes to system capabilities for ... (g) Introducing data for a vote not cast by a registered voter.” I would rather the system simply prevented such votes, as I hope was the intent! As written, the rule permits there to be authorized change to the capability to prevent such votes.

Rules 45.5.2.7.2 and 45.5.2.7.3 cite “the State’s *Minimum IT Architecture Standards*.” These are documented in Rule 1-3 of the State’s Information Technology Management Code [5]. (Paradoxically, the subsections of Rule 1-3 are numbered as section 7.) Section 7.1.1 requires that “all state computers be accessible via an IP network.” IP, in this context, refers to the Internet Protocol, as is made quite plain in everything that follows. Much of the remainder of this document deals with the administrative and security problems posed by this requirement.

While this requirement is clearly reasonable for some computers, it is not at all clear that voting machines should ever be connected to the Internet. All modern voting machines and ballot tabulating machines contain computers. Rule 7.2.3 states that “every state datacenter must provide network access...” This is in direct conflict with a common design for secure election data centers, where a commonly recommended practice is to require that the election management

system computers have no network connections in order to ensure that they cannot be infiltrated. Rule 7.8.3 demands virus detection mechanisms, which is well and good, but it ignores the fact that there are other defensive measures that can be taken, including system designs that are inherently immune to such attacks. Rule 7.8.4 requires encryption for wireless data, but where public records such as polling place election results are being transmitted, encryption serves no purpose. In such cases, strong document authentication is what is needed.

Another way to go about assessing the adequacy of Colorado's voting system assessment is to read copies of the *State of Colorado Voting Equipment Qualification Report* for several voting systems. I reviewed the reports for Diebold [6] and Sequoia [7]. Those parts of these reports dealing with evaluation of system usability from a county election official's perspective are useful. The certification exceptions and warnings in sections III and IV of each report is well presented. The general comments are useful, and in cases where I have also worked with the same voting system, they match comments I might have made.

On the other hand, the material found in appendices F through H of each certification report is inadequate. This is also known as Forms 8.1 9.1 and 9.3. The central problem with these forms is that they are mere checklists. Appendix F, form 8.1, for example, lists 116 different documentation requirements. If the vendor provides documentation of the necessary requirement, the requirement is considered to be satisfied. Given the size of each vendor's technical data package, it should have consumed a considerable amount of time to find what document or documents satisfied each of these requirements; however, the matrix does not record what document or documents contained the required information. I cannot tell from the handwritten notes on this form what documents were deemed to satisfy which requirement or how carefully those documents were assessed. The Sequoia document [7] includes many handwritten section numbers, but these are not easy to tie to particular documents provided by Sequoia.

In looking at these copies of Appendix F, about half of the entries merely contain the handwritten notation P, indicating passed. The second most common entry is an F crossed out and replaced by a P, with no evidence of the grounds on which the initial F was given or the grounds on which it was changed. Illegible handwritten notes are also common. Occasionally, the state's examiner, John Gardner, has added machine-printed notes, but these do not clarify the situation.

John Gardner testified that he maintains logs of the testing procedure on record with the Secretary of State, and that Appendix G and H are this log (page 118 line 5 to page 119 line 9 of [3] Volume I). These forms, with their scrawled notes and vague descriptions of tests, do not satisfy my understanding of the requirements of Rule 45.6.2.2.3 of [2], particularly with regard to test descriptions. I suspect that scores marked F and changed to P are related to deviations, for which Rule 45.6.2.2.5 leads me to expect significant (and readable) discussion of what happened.

Appendix G, also known as Form 9.1, is a demonstration checklist. Indeed, many voting system requirements can be satisfied by demonstration. This is the case when the requirement asks for a feature to be present and where mere observation of a demonstration of that feature is sufficient to verify correctness. For some of Colorado's requirements, demonstration is not sufficient. The very first requirement here, 45.6.1.2(a) "Demonstrate the System Overview" and the last (p) "Troubleshooting problems throughout the process" are the most troublesome. Can an overview be demonstrated? What criteria apply to an evaluation of a demonstration of troubleshooting?

Appendix H, also known as Form 9.3, is another checklist for the cumulative results of the general testing matrix. This form lists 195 "tests", of which well over 100 are described as being "Demo" tests. This leads to the obvious question, how is the testing documented in Appendix H different from that in Appendix G? Some of this material is so vague that I could not discern any evaluation criteria for many of the "tests", yet Colorado's statutes and administrative rules certainly led me to expect criteria. For example, "9.3.2.23, Verify the following performance standards" appears

objective only until you realize that the time limits set for the 4 sub-parts of this “test” depend on the complexity of the ballot under test. Or consider “9.3.4.12, [part 2] Demonstrate and record all error messages for the device.” This is an open-ended test that could go on for days, because some error messages are extraordinarily difficult to elicit.

Of greater importance, many of the demonstrations asked for in Appendix H require the demonstration of negatives. For example, consider “9.3.2.10 Demonstrate ... that third party hardware and software does not impact performance levels ...” In general, no finite demonstration can possibly demonstrate that there is no impact. Rather, the most that can be demonstrated is that, for the cases tested, on the occasion of those tests, no impact was observed. This is a problem for “9.3.3.2 Devices shall have unique locks and keys ...” and 9.3.3.5 to 9.3.3.14, each of which begins “demonstrate the systems' ability to prevent unauthorized changes to ...”. The problem also appears in 9.3.4.26, 9.3.4.30, 9.3.4.32, 9.3.4.51, 9.3.5.8, 9.3.7.19, 9.3.8.13, 9.3.8.14, and probably others.

I am particularly concerned that the majority of the security requirements have been boiled down to “tests” requiring the demonstration of a negative. In fact, a large fraction of the negative demonstrations I have listed above have serious security consequences. Where the state law requires that the secretary of state adopt rules establishing minimum standards for security requirements ([4] CRS 1-5-616 (1) (g)), and where these requirements state that “at no time shall the system allow for unauthorized changes to system capabilities for defining ballot formats” ([2] Rule 45.5.2.6.1 (a)), all that is actually being tested is that in the case demonstrated, the system prevented an unauthorized attempt to change a ballot format. John Gardner described these “tests” in a way that confirms my conclusions about their inadequacy (page 121 line 15 to page 122 line 11 of [3] Volume I). Such an effort cannot be properly described as a test.

Opinion Regarding the State's Inability to Assess Documents

The state must prevent release of critical information that would allow interference with the correct and honest conduct of elections. For very practical reasons, the state must also ensure that voting system vendors' proprietary rights are not compromised, least the vendors decide not to sell voting systems in Colorado. These legitimate reasons for withholding documents from the public compete with a general public right to know that is necessary if the public are to be able to assess the honesty and competence of their government.

The Modified Stipulated Protective Order [8] under which I was able to examine the vendor technical data packages creates two classifications, “Confidential Information,” that “contains, reflects or concerns trade secrets or other proprietary information,” and “Security Information,” “the dissemination of which could compromise the security and proper functioning of the electronic voting systems.” These two categories are entirely appropriate and conform to my understanding of the state's ethical responsibilities in this case. Except in cases where the state had insufficient time to mark documents according to these classifications, documents containing “Confidential information” were rubber stamped CONFIDENTIAL and documents containing “Security information” were rubber stamped EYES ONLY. Where time constraints precluded stamping, clear verbal notice was always given of the status of the documents.

The FEC 2002 Voting System Standards [9], in Volume II section 2.1.3, compels the vendor to clearly mark all documentation containing proprietary information as such. It is extremely rare to find any criticism of vendor decisions to mark information as proprietary, and as a result, most vendor documentation is indiscriminately marked as proprietary, whether or not it actually discloses anything at all. In Colorado, the state appears to have uncritically accepted the vendor's markings, without regard to either the content or intended distribution of the material.

John Gardner has testified that he was not aware of which if any of these documents was available to the public, that he made no effort to do so (page 131 line 6 to page 133 line 10 of [3] Volume I). Given that John Gardner has testified that he does not normally read these documents (page 137 line 5 to page 138 line 19 of [3] Volume I), and specifically, that he does not read ITA documents (page 357 lines 10 to page 360 line 6 of [3] Volume II). As such, I would expect his document classification decisions to be arbitrary, and that is, in fact, what I observed.

Consider, for example, the state's treatment of documents describing printing requirements for optical mark-sense ballots. Diebold's *Ballot Specifications* [10] were marked CONFIDENTIAL, while the corresponding document for Sequoia, the *Optech Ballot Printing Specifications* [11] were marked EYES ONLY. In fact, anyone who requests an absentee ballot can, at their leisure, measure the details of the ballot and infer most of this information quite easily. Furthermore, the sample ballots many jurisdictions post on their web pages reveal even more, as many of these are the actual PDF images sent to the ballot printer, overprinted with the words *sample ballot*. As a result, this information is in no way security critical or even proprietary.

Similarly, documents describing the formats of public records cannot possibly be security critical, as anyone who goes to the effort of obtaining those records can infer the format. Thus, I was astounded to find that the collection of sample reports from the Optech Insight [12] was redacted, and then restored and marked EYES ONLY. I would suggest that wherever there are public records, any documents necessary to interpret those records must themselves be public. If we accept anything less than this, the records involved are not really public.

Another example is provided by the classification of material from the Independent Testing Authority (ITA) reports on these voting systems. All of these reports made available by the state were marked EYES ONLY and heavily redacted. In the case of Diebold, there were a total of 6 reports, three from Ciber, Inc. [13] [14][15], and three from Wyle Labs [16][17][18]. Of these, all but one report from Ciber [14] is currently available on the Internet. Of these publicly available copies, two have no redactions [15] [16], while the others have line numbers and source code quotations redacted. If the state genuinely believes that these reports contain information "the dissemination of which could compromise the security and proper functioning of the electronic voting systems" (quoted from the Protective Order [8]), then the presence of these reports on the Internet, it would seem, brings into question any use of Diebold's systems in Colorado.

Public curiosity and suspicions raised by reports about the security of Diebold voting systems have led to a large number of public document requests involving Diebold. I have no reason to believe that ITA reports for other vendors would not be equally available if a sufficient number of public records requests were filed in a sufficient number of states. My understanding of New York's new voting system standards, for example, suggests that they intend to place all ITA reports submitted to New York on the state web site. Similarly, my understanding of the newly revised Federal process suggests that they intend to place ITA reports on the web by the summer of 2007.

In general, neither the ITA reports I have read for this case, nor the ITA reports I read as an examiner for the state of Iowa contained security critical information, except when they disclosed the existence of significant security flaws in voting systems. In those cases, I have always hoped that we could find a way to enforce our voting system standards to prevent the use of such flawed systems. Unfortunately, to date, this has not been the case.

It is fair to ask what level of security voting systems should be held to. I and many others have long recommended that voting system security be considered a matter of national security because of its critical role in our democracy. If we are to hold voting systems to this standard, we must reject the sloppy security practices that dominate the personal computer marketplace and consider the far more stringent norms that the military and national security apparatus have long

advocated.

In the documents I reviewed with titles containing the word "security" I found no critical security information. I reviewed such documents for the Sequoia Optech Insight [19], the Sequoia Optech 400-C [20], the Sequoia AVC Edge [21], and WIN EDS [22]. It is noteworthy that several of these documents acknowledge their creation in response to section 2.6.2 of Volume II of the FEC 2002 Voting System Standards[9]. The Optech 400-C, for example, is a product that dates back at least to the mid 1990's, so I would have hoped to find a real security specification with a revision history that traced back to that era. This is not the case. I found no similar gratuitous security specifications among the Diebold documents I examined.

In my opinion, all of the above-cited security documents could be released to the general public, yet all were marked EYES ONLY. The only confidential information they contain is *the bare fact of their shallowness*. Advice to store equipment securely [19] is not critical, nor is the fact that the Optech 400-C uses a widely used secure hash function to protect data integrity [20], nor is the fact that the AVC Edge uses a mix of pseudo-random numbers and data from the system clock in order to shuffle ballot data in its internal memory, nor is the fact that WIN EDS uses 5-bit access permission codes [22].

Similar comments can be made about numerous other documents. The Diebold Election Administrator's Guide [23], for example, was originally marked CONFIDENTIAL with heavy redaction. When the redactions were withdrawn, large parts of this document were marked EYES ONLY. In fact, this document merely walks the reader through normal and reasonable administrative controls for a county election management system, essentially all of which follow naturally from a introductory description of the system. The security control forms given here are of no importance when blank; it is only when they are filled in with the actual keys and passwords used in a particular county that they become security critical.

A similar document category are those documents dealing with quality assurance and testing. Sequoia produced such documents for the Optech Insight [24], the Optech 400-C [25][26], and the AVC Edge [27]. In my opinion, none of these documents contained any information that was security critical or even worthy of being considered proprietary. Paradoxically, the state classified one of these documents as CONFIDENTIAL with no redactions [25], released another as CONFIDENTIAL in heavily redacted form and then rescinded the redactions, marking them EYES ONLY [24], and released two duplicate copies of another, both marked CONFIDENTIAL, but only one redacted [26]. The remaining report was only released in EYES ONLY form [27].

I examined the pollworker's guides for the AccuVote OS [28] and the AccuVote TSx [29]. Both were marked CONFIDENTIAL. In general, I cannot understand why pollworker manuals are considered confidential. These manuals are widely distributed. I estimate that there is about one pollworker for every hundred people who vote in a general election, and essentially all of these pollworkers are temporary employees who are subject to minimal screening. As a result, I would consider it dangerous if a pollworker's guide contained security critical information and I consider the effort to limit the distribution of pollworker's manuals to be inherently doomed. Furthermore, election observers really cannot be expected to assess the behavior of pollworkers without access to these manuals. The discussion of security in these guides focuses on procedures that observers ought to be aware of and ought to be able to verify to have been properly conducted.

Opinion Regarding Diebold Products

Had the state set standards in conformance to the statute, requiring that the documents submitted by the vendors be evaluated, and had the state set competent voting system examiners to work reading these documents, they would have found some serious reasons for concern. The documents submitted by Diebold should have raised serious questions about the security of

Diebold's products. The central problems exposed here involve distribution of security keys, a home-grown access control mechanism, the security of ender cards under AccuVote OS, the pervasive use of Internet protocols, and ineffective mechanisms for software version control and verification. In addition, even a cursory reading of the ITA reports reveals that there are additional problems.

On November 6, 1997, at a meeting of the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems, I discovered that Diebold's corporate predecessor, Global Election Systems, was selling a voting system where every machine they used relied on the same fixed key for encryption. Diebold appears to have finally fixed this problem. As I understand their solution, it involves use of special smart cards called *key cards* that are used to distribute security keys to the various pieces of voting equipment used in an election. These cards interact with VC Programmer [30], Key Card Tool [31], the AccuVote TSx [32] and AccuVote TS [33], and the Vote Card Encoder [34]. It is very clear that these cards form a critical part of the security of the AccuVote TSx.

My first concern is that, despite the automation provided by such tools as the Key Card Tool, Diebold's system of key cards is, essentially, a manual system. The paper forms used are documented in the Election Administrator's Guide [23], section 4.12. This material was originally redacted and restored marked EYES ONLY. There are two distinct problems with this material. First, the user is expected to write down passwords and cryptographic keys on these forms and then file them safely. One of the oldest rules in computer security is to never write down passwords and to use them sufficiently sparingly that writing them down is rarely appropriate. It follows that systems where users are instructed to write down large numbers of passwords are not a good idea. Furthermore, it appears that election administrators are being called on not only to invent passwords, but also to invent the cryptographic keys themselves. This is bad. People are not good at inventing truly random keys, and as a result, the security of documents keyed with human-generated keys is usually far less than the security of documents keyed with random keys.

My second concern with this centers on the security of the key cards themselves. I did not find any documents that described the implementation of key cards in sufficient detail that I could evaluate their security or insecurity, nor did I find any documents that suggested that the security of these devices had been assessed in any way by the State of Colorado. The state should have asked how hard it would be to forge a key card and use it to re-key a voting machine and how hard it would be to copy a key-card. To fail to do this in the presence of explicit legislative mandate to set security standards is wrong.

There is ample evidence that Diebold has opted to invent their own access control mechanism. There is evidence of this in the GEMS User's Guide [35] (AG7336-38) where, both in the numerous special screens devoted to this, and in the overuse of password protection on objects where this is not appropriate. This problem is even worse, though, with the Sequoia system, so I will discuss it there.

The AccuVote OS documentation raises a number of concerns. First among these is the presence of a specially encoded "ender card", mentioned in the Pollworker's Guide [36] and the Hardware Guide [37]. The encoding that indicates that an "ender card" is indeed such is given in the Hardware Guide (AG7643) and the Pollworker's Guide explains the trick required to close the polls using the ender card. The Hardware Guide also documents additional odd card types such as a card that, if fed through the scanner, causes it to start counting ballots as absentee ballots. On observing the existence of these special cards, I would expect a security evaluation of the AccuVote OS to include a section evaluating the consequences of such a card falling into the hands of a voter and the protective measures taken, in the design of the system, to prevent such an event leading to trouble. In addition, I would have expected a pointed question to be asked to the vendor: Does the system support any undocumented card types? I ask this because Michael

Shamos (Pennsylvania's voting system examiner) has told me the story of finding that one vendor supported numerous undocumented special card types, including some that would make arbitrary adjustments to vote totals.

Voters are regularly assured that voting systems cannot be connected to the Internet, but the Diebold documentation contradicts this. The Central Count User's Guide [38] shows how to connect the machine to the Internet (AG7708-20), including how to set up the IP (Internet Protocol) address and how to configure it for an Internet ISP (Information Service Provider). The Precinct Count User's Guide [39] documents similar material (AG8258-61) and makes it clear that the modem connection can be used, in conjunction with a remote computer, to arbitrarily program the memory card loaded in the machine. The AccuVote TS [33] uses the SSL communications protocol (AG8383). Furthermore, the TS may have its IP address, network ID and password assigned from the screen (AG8394-5), implying that it can easily be connected to the Internet through any Internet service provider to any computer anywhere. With this extensive use of Internet communication protocols throughout the product line, a security analysis must examine, at the very least, the security consequences of this. In Colorado, however, more is required. These systems must be brought into conformance with the state's Information Technology Management Code [5]. I see no evidence that the state has enforced this requirement.

The GEMS System Administrator's Guide [40] continues with this pattern and raises another issue. There are several ways to transmit passwords in setting up Internet connections, and Diebold supports several of these, including the most dangerous, transmission of unencrypted passwords in a form that any eavesdropper can decode (page 5-14). The state should have noticed this and issued a clear warning to the counties forbidding the use of this option.

Several Diebold manuals speak of version verification and assurance, that is, methods to assure or verify that the software or firmware running on a particular piece of voting equipment is the version that was approved for use on that equipment. The GEMS 1.18 Administrator's Guide [40] (AG6245-69) gives an elaborate checklist that purports to offer some assurance. The AccuVote TS User's Guide [33] (AG8383) offers a brief discussion of this issue. In sum, the general approach relies on self-reporting, by the software, that it is the correct version, combined with human effort to assure the chain of custody on all systems so that the wrong version is never allowed to be installed. Given the widespread problems reported in other states with voting systems running the wrong software or firmware version, the state should be wary of placing such a high burden on voting system administrators.

Finally, there is the issue of the ITA reports on the Diebold system. A close reading of these reports reveals numerous problems. The Ciber Software Functional Test Report on GEMS 1-18-24 [13] cites on page 10 a Diebold document that should be of interest to anyone attempting to assess the quality of Diebold's software and firmware, *Diebold's C++ Coding Style Version 2.0*. I have seen no evidence that the state was aware of or requested access to this document. Another statement on page 10 is simply false: "Gems 1.18.24 uses C++ code The C++ language facilitates and enforces the object oriented design" It is true that C++ facilitates object oriented design, but it in no way enforces it. This appears to be an example of overuse of boiler-plate language by the ITA, one that seriously detracts from their credibility.

The Ciber Source Code Review and Functional Testing [15] is particularly important. This report was prepared at the request of the State of California after its own Voting Systems Technology Assessment Advisory Board (VSTAAB) released a study showing major flaws in the Diebold AccuBasic Interpreter [41]. This Ciber report confirms, in large part, the negative conclusions of the VSTAAB report. This widely available report says that the system can be used, but it couches this in wording that should warn the reader that things are not right, for example: "The fact that programs appear to provide adequate security shall not be interpreted to mean that the programs are not without security vulnerabilities." In sum, they found that, all versions of the Diebold

AccuBasic interpreter, which is part of the AccuVote OS, TS and TSx products, contained significant flaws. The report goes on to say that in the case of the TSx, but not the others, there is "a check to validate the AccuBasic object files, so that if a file is tampered with, no tampering will be detected." Unfortunately, the report does not give any indication that the efficacy of this check was assessed. To carry out its responsibility to set security standards, the state of Colorado should have demanded further information from Diebold to allow the efficacy of this check to be assessed.

The Wyle Change Release Report for Firmware Release 4.6.4 [16] page 9 lists many errors that were corrected from previous versions of this software. As a general rule, when I see the list of errors corrected in a new software release, I find it safe to assume that the new release contains similar errors. I am worried, therefore, when I find errors as severe as "corrected incidence of inactive timeout page appearing randomly when voting or printing ballots" in a version with a version number that suggests considerable maturity. One change "Randomized upload ballot order" reflects a fix to a bug that was reported in August 2003. It should have been fixed immediately and certainly before November 2004, since this has an effect on voter privacy. The state should, at the very least, have asked for an assessment of the quality of the ballot order randomization used.

It is alarming that this Wyle report claims to have inspected the AccuBasic interpreter (page 7, reference to Abasic, page B6, reference to file abinterp.c) and claims to have tested the software for robustness and security (page 11), yet found none of the problems that Ciber or the VSTAAB would find only a few months later. The earlier evaluation of Version 4.6.1 [18] also indicates examination of the AccuBasic Interpreter (page A-34, file abinterp.cpp), so there is ample evidence that versions of this software component have been routinely examined without finding more than cosmetic errors.

The Wyle Report on the AccuVote OS Firmware [17] includes a test matrix that lists numerous test categories that were declared, by Wyle, to be not applicable or not tested. The requirements for data integrity during telecommunication and for use of public networks were not tested (6.5, 6.6.1 pages A-31 to A-32). Given that the AccuVote OS uses the IP protocol suite, as discussed previously, it is alarming to find this entire category of requirements has been ignored. The state should have noticed this. To carry out its responsibility to set security standards, the state should have forbidden connection of the AccuVote OS to any networks, public or private, pending testing of the requirements in 6.5, and it should have forbidden connection to a public telecommunications network pending testing of the requirements in 6.6.1.

There are serious questions about the use of Microsoft Windows CE in the Diebold AccuVote TSx system. I first asked questions about this issue when the Global Election Systems AccuTouch system, the ancestor of the AccuVote TSx, came before Iowa in 1997. At the time, it used Windows 95, and it was obvious that this COTS product has been modified for use in the voting machine. I was assured that these modifications were trivial. Unfortunately, the fact that a modification is trivial does not exempt it from examination under the 1990 or 2002 voting system standards. Since that time, with the shift from Windows 95 to Windows CE, these trivial modifications have grown large, and I see no evidence in any of the relevant ITA reports [16][18] that the ITA, Wyle labs, in this case, has properly examined Diebold's customizations to Windows CE. Richard R. Lee has written about this in more detail, and I concur with his assessment [50].

Opinion Regarding Sequoia Edge II

The most striking characteristic of the Sequoia documentation is the sheer volume of paper involved. On reading into this paperwork, I was struck, again and again, by how much of this was apparently written with no intent that it ever be read by anyone. The Optech Insight Security Specification [19] is not even complete. Section 5.6.2, on pages 5-3 and 5-4, is just an outline,

ending with a bullet “Security vs. the Public Right to Know.” Indeed, someone should write this. The AVC Edge Software Technical Description [42] (638 pages) and the HAAT documents [43] (1896 pages) are massive piles of near useless documents, apparently produced in some semi-automatic way from source code file headers, based on the pattern set by the archaic on-line documentation system that has been distributed with the Unix operating system since the mid 1970s. The WinEDS Software Specification [44] is, put simply, not a useful software specification, but merely a collection of screen shots and largely redundant prose. The Software Development Checklist at the end of this document (AG11752) would get a student laughed out of an undergraduate course in software engineering.

We can infer, from the Optech 400-C Change Release Summary for Version 1.10 [45] that the firmware for this system is written in C++, using makefiles to control software builds, and using CVS for version management. While this is not the most advanced software development environment, it is certainly appropriate for continued development of a product as old as the Optech 400-C. In contrast, we find, in a corresponding document for the Edge [46], that the version numbers are being incremented by hand as late as November 2005. This suggests that the software development tools being used to manage different products in the Sequoia product line operate at vastly different levels.

I have already commented on the fact that Sequoia's security specifications [19][20][22] are not, in any useful sense, security specifications. I believe that all of these largely vacuous specification documents were written after the fact, in response to the FEC 2002 voting system standards [9]. There is a considerable literature on how to write useful security documents. Consider, for example, the tutorial documenting reasonable practices in this arena is available from the National Institute of Standards and Technology web site [47].

While Sequoia's “specifications” come nowhere near best practices, they do reveal some problems. The Insight Security Specification [19] states (on page 4-1)

REDACTED

These raise a very important issue that is not answered in any of the documentation I have read. A competent security assessment will ask how the Sequoia products verify that they are running the correct software versions.

There is ample evidence that, like Diebold, Sequoia has built their own access control mechanisms, apparently from scratch. This is made clear in the Software Specification for the Edge/Advantage [44] sections on Security (AG11543-6), Interfaces (AG11623-7), G.2.1 Security (AG11662), and N.7 Security (AG11731). The WinEDS security specification [22] documents the encodings they have used for access rights in their system (pages 2 to 4). In general, finding that a vendor has opted to build elaborate security mechanisms on top of an operating system instead of using the native security mechanisms of that system is alarming. As a rule, such after-the-fact security systems invariably turn out to be full of holes. The evaluation of the security of a homebuilt access control system must rest on a clear understanding of these risks. I see no evidence that the state's evaluation noticed any of these issues.

One justification for developing their own access control mechanisms would be the “legacy system” argument, which states that they must live with the legacy of systems they have inherited from corporate predecessors such as Business Records Corporation, the original maker of the Optech family of products. This argument would hold water if there were no adequate security systems available decades ago, but this is simply not true. While the security models of the older versions of Microsoft's Windows family of operating systems was laughable, Windows NT became available in 1993, and the first commercial distribution of Linux dates to the same year. Both of these systems have always supported generally competent access control models. Other

operating systems supporting adequate access control models date back into the early 1970s. Under these circumstances, a vendor's decision to build from scratch is usually evidence of serious misunderstandings of what can be done with the mature access control mechanisms that are currently on the market.

The documentation of the Audio Accessory for the AVC Edge [48] contains a bombshell. Again and again, the text of the audio messages for blind voters refer to the buttons by color (AG12332). True, the buttons are always described in terms of color and shape, but there are two triangular buttons distinguished only by orientation and color, so the reference to the yellow triangular button is not helpful. I have heard from several blind voters who were deeply offended by this misfeature, and I find it remarkable that it was not noticed in Colorado's testing.

The ITA report for the Optech Insight [49] raises a major question. Section 4.2.1 states

REDACTED

This divided architecture, with half of the software on removable media, may create a significant vulnerability for injection of viruses or other malicious software through interchange of removable media between machines. The division also creates a situation where the HPX is a shared operating environment, shared between different APX versions created for different elections. In conjunction with the weak documentation of the software integrity checks in the Security Specification [19] (page 4-1), this cries out for investigation. Yet, in the ITA report, Appendix A, a testing matrix is given that indicates that there was no assessment of protection against malicious software (6.4.2) or of a shared operating environment (6.5.5). In the limited time available, under the documentation access constraints I was faced with, and with the sheer volume of Sequoia documentation was unable to pursue this. A competent state security evaluation must consider such questions.

INFORMATION CONSIDERED

A list of the materials that I have reviewed and considered in forming my opinions in this case, in addition to my familiarity with the scientific literature, is attached as Appendix A.

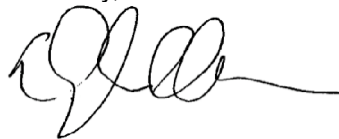
OTHER TESTIMONY

During the past 4 years, I testified only once, in a video deposition taken in Troy, Missouri on September 22, 2002, in a case filed by Gregory Allsberry against Lincoln County.

COMPENSATION

I am not compensated for my services in this matter as an expert witness. I am volunteering my time because the issues in this case are fundamental to democracy.

Sincerely,

A handwritten signature in black ink, appearing to read 'Douglas Jones', with a long horizontal line extending to the right.

Douglas Jones, Ph.D.

APPENDIX A: Documents Reviewed

[1] In Re: Complaint of Al Kolwicz Concerning Hart/Intercivic eSlate Voting Equipment. Secretary of State Complaint: SOS-HAVA-01-06-0001, July 10, 2006.

[2] Election Rules of the Colorado Secretary of State.

[3] Deposition of John H. Gardner, Jr. -- Volume I, August 29, 2006 and Volume II, August 30, 2006, prepared by Patricia S. Newton.

[4] Colorado Revised Statutes, Section 1-5-616 and 1-5-617.

[5] Information Technology Management Code, Colorado Commission on Information Management, Governor's Office of Innovation and Technology. 2006.

[6] State of Colorado Voting Equipment Qualification Report -- Diebold Election Systems, 2005-CDOS-DIE-001-1123, May 30, 2006.

[7] State of Colorado Voting Equipment Qualification Report -- Sequoia Voting Systems, 2005-CDOS-SEQ-001-1228, May 30, 2006.

[8] Modified Stipulated Protective Order, Conroy vs Dennis, August 11, 2006.

[9] Federal Election Commission, 2002 Voting System Standards, available on the web from http://www.eac.gov/election_resources/vss.html

[10] Diebold Election Systems, Ballot Specifications, AG7274.

[11] Sequoia Voting Systems, Optech Ballot Printing Specifications.

[12] Sequoia Voting Systems, Optech Insight Sample Reports, Version 1.00, September 2005. AG12087.

[13] Software Functional Test Report -- Diebold Election Systems -- GEMS 1-18-24, Original Report Version 1.0, created 08/03/05, Cyber, Inc. Available on the Internet with one small redaction at <http://www.bbvdcs.org/stash/Ciber-db-gems1-18-24.pdf>

[14] Addendum to Software Functional Test Report -- Diebold Election Systems -- GEMS 1-18-24, Cyber, Inc., Sept. 30, 2005.

[15] Diebold Election Systems, Inc. Source Code Review and Functional Testing, Cyber, Inc., February 23, 2006. Available in on the Internet, un-redacted, form www.ss.ca.gov/elections/voting_systems/diebold_code_review_final.pdf

[16] Change Release Report of the Diebold Election Systems AccuVote-TSx DRE Voting Machine with AccuView Printer Module (Firmware Release 4.6.4), Wyle Laboratories, Report No 52501-01, November 14, 2005. Available on the Internet, un-redacted, form from http://www.bbvforums.org/forums/messages/2197/Wyle_Lab_4_6_4_00001-32747.pdf

[17] Hardware Qualification Testing of the Diebold Election Systems AccuVote Optical Scan Model D Precinct Ballot Counter (Firmware Release 1.96.6), Wyle Laboratories, Report No 48619-09, August 4, 2005. Available on the Internet with line numbers and quotations from source code redacted in Appendix B in two parts from <http://www.bbvdocs.org/stash/wyle-diebold-1.96.6-hdwr.pdf> and <http://www.bbvdocs.org/stash/wyle-diebold-1.96.6-pt2.pdf>

[18] Functional Qualification Testing of the Diebold Election Systems VCPProgrammer and Key Card Tool (BallotStation Firmware Release 4.6.1), Wyle Laboratories, Report No 48619-10, August 4, 2005. Available on the Internet with line numbers and source code quotations redacted in Appendix A from http://www.bbvforums.org/forums/messages/2197/wyle1-96_6-23144.pdf

[19] Sequoia Voting Systems Optech Insight Security Specification, Version 1.01, September 2005.

[20] Sequoia Voting Systems Optech 400-C Security Specification, Version 1.00, March 2004.

[21] Sequoia Voting Systems AVC Edge Security Overview, Release 5.0, 5/10/05

[22] Sequoia Voting Systems Win EDS for AVC Advantage Security Specification, Release 3.1, Version 1.03, December 2005. AG11794.

[23] Diebold Election Systems GEMS 1.18 Election Administrator's Guide, Revision 9.0, June 27, 2005. AG6318.

[24] Sequoia Voting Systems Optech Insight Quality Assurance Program, Version 1.01, September 2005. AG11828.

[25] Sequoia Voting Systems Optech 400-C Quality Assurance Program, Version 1.00, March 2004. AG11828, AG12020 (2 identical copies).

[26] Sequoia Voting Systems Optech 400-C Test & Verification Specification, Version 1.02, January 2005. AG11924 (un-redacted version), AG11972 (redacted version).

[27] Sequoia Voting Systems AVC Edge Quality Assurance Program, Version 1.00, May 2005.

[28] Diebold Election Systems AccuVote OS Pollworker's Guide, Revision 3.0, February 18, 2005. AG7573.

[29] Diebold Election Systems AccuVote TSx Pollworker's Guide, Revision 5.0, March 22, 2005. AG7996.

[30] Diebold Election Systems VCPProgrammer 4.6 User's Guide, Revision 1.0, April 3, 2005. AG7245.

[31] Diebold Election Systems Key Card Tool 4.6 User's Guide, Revision 1.0, April 13, 2005. AG7776.

[32] Diebold Election Systems AccuVote TSx Hardware Guide, Revision 8.0, February 19, 2004. AG7796.

[33] Diebold Election Systems Ballot Station 4.6 User's Guide, Revision 1.0, March 22, 2005. AG8372.

- [34] Diebold Election Systems Vote Card Encoder, Revision 1.0, February 10, 2004. AG7966.
- [35] Diebold Election Systems GEMS 1.18 User's Guide, Revision 12.0, August 21, 2005. AG7292.
- [36] Diebold Election Systems AccuVote OS Pollworker's Guide, Revision 3.0, February 18, 2005. AG7573.
- [37] Diebold Election Systems AccuVote OS Hardware Guide. AG8521.
- [38] Diebold Election Systems AccuVote OS Central Count 2.00 User's Guide, Revision 4.0, September 17, 2004. AG7591.
- [39] Diebold Election Systems AccuVote OS Precinct Count 1.96 User's Guide, Revision 4.0, February 17, 2005. AG8113.
- [40] Diebold Election Systems GEMS 1.18 System Administrator's Guide, Revision 6.0, April 21, 2005. AG6223.
- [41] David Wagner, David Jefferson and Matt Bishop, *Security Analysis of the Diebold AccuBasic Interpreter*, California Secretary of State's Voting Systems Technology Assessment Advisory Board. Available on the Internet from http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf
- [42] Sequoia Voting Systems AVC Edge Software Technical Description, Release 5.0, 2005.
- [43] Sequoia Voting Systems HAAT (Hybrid Accumulator & Transmitter) documents.
- [44] Sequoia Voting Systems WinEDS for AVC Edge/Advantage Software Specification, Release 3.1, Version 1.07, December 2005. AG11477.
- [45] Sequoia Voting Systems Optech 400-C WinETP Change Release Summary Version 1.10, March 2004. AG12147.
- [46] Sequoia Voting Systems AVC Edge Change Release Summary, Version 5.0.19, 10 November 2005. AG12207.
- [47] Tim Grance, Joan Hash and Marc Stevens, *Security Considerations in the Information System Development Life Cycle*, Recommendations of the National Institute of Standards and Technology, Computer Security Division, NIST Special Publication 800-64, Rev. 1. June 2004. Available on the Internet from <http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>
- [48] Sequoia Voting Systems AVC Edge Audio Accessory Pollworkers/Operators Manual, Revision C, Release 5.0, October 2005. AG12318.
- [49] Preliminary Qualification Testing of the Sequoia Optech Insight Precinct Ballot Tabulator Release APX K2.08/HPX K1.42, November 4, 2005.
- [50] Richard R. Lee, Expert Report / Conroy et al v. Dennis, September 1, 2006.

NOTE added after redaction: Numbers of the form AGxxxx are Bates numbers. They represent page numbers, so if you know the Bates number of the title page of a document and the bates number of a citation in that document, you can find the cited page by taking the difference and then turning that many pages.