*Approved for public release by Secretary Dennis and the Colorado Attorney General (who partly redacted this report)*

Dan Wallach
Rice University
6100 Main St.
Duncan Hall 3121
Houston, TX 77005-1892

September 5, 2006

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

RE: *Conroy et al. v. Dennis* – Expert Report

Dear Mr. Efaw:

This is my report in the Colorado Direct Recording Electronic ("DRE") voting systems case, *Conroy v. Colorado Secretary of State Ginnette Dennis.*

## I. QUALIFICATIONS

My expertise is in computer security, in which I have been performing research since 1995. As a graduate student at Princeton University, I helped find significant flaws in Sun's Java system, then being adopted widely in web browsers, which would allow a hostile web page to completely take over a web surfer's computer. Later, as a professor at Rice University, I have studied security issues that arise in a number of networked systems, including flaws we found in Google's Desktop Search, which would allow an outsider to see the results of local searches.

I first considered electronic voting security issues after Harris County, Texas, adopted Hart InterCivic's paperless eSlate system in 2001. Because I live in Harris County, and because I was known locally for my work in computer security, I was asked to testify before the Houston City Council about whether I felt this was a good idea. My opinion then, as now, is that paperless electronic voting systems introduce a wide variety of security issues to elections that appear to not have been given serious consideration by either the vendors or the state or federal certification standards. More recently, voter-

verifiable paper audit trail (VVPAT) systems have improved the situation with electronic voting in some States, but important security concerns remain even where VVPAT systems are used.

Since 2001, I have published three research papers on electronic voting security issues; I have testified about voting issues to government agencies across the U.S., as well as internationally; I have assisted National Institute of Standards and Technology (NIST) and the U.S. Election Assistance Commission (EAC) in the drafting of the 2005 federal Voluntary Voting System Guidelines; and I have assisted the Carter-Baker Commission on Federal Election Reform and the Brennan Center's Voting System Security Task Force. I am also the associate director of ACCURATE (A Center for Correct, Usable, Reliable, Auditable, and Transparent Elections), which is a research center funded by a $7.5 million grant from the National Science Foundation and which studies technological and policy issues with voting systems.

A copy of my curriculum vitae, including a list of my publications, a complete bibliography and a list of litigation matters in which I have been engaged, is attached to this report as Exhibit A. My qualifications to testify as an expert witness in the fields of computer security generally and voting technology specifically are provided in that document.

## II. OPINIONS

### A. Summary of Opinions

In this matter, Wheeler Trigg Kennedy LLP, on behalf of Plaintiffs, retained Dr. Douglas Jones and I as expert consultants on computer security and voting technology issues. Dr. Jones and I have divided the labor such that he primarily has considered documents relating to voting systems manufactured by Diebold and Sequoia, respectively, whereas I considered documents relating to voting systems manufactured by ES&S and Hart InterCivic. As such, many of my opinions focus on those latter two vendors. In other instances, I offer general conclusions that apply to all four of the subject vendors.

My opinions in this matter are based on my education, training, study, and experience in the fields of computer science and voting technology. My opinions are expressed to a reasonable degree of scientific 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.

Broadly stated, I believe that the Colorado Secretary of State's voting-system certification policies and procedures lack the necessary sophistication and depth to determine whether a voting system vendor's equipment is secure in any meaningful sense, and that Colorado's certification process is highly unlikely to detect important security flaws in the subject Direct Recording Electronic (DRE) voting systems. Most strikingly, the Secretary of State has failed to promulgate any minimum standards for computer security and appears to have delegated all responsibility for such minimum

standards to the four vendors whose systems are involved in this case. Further, I believe that the Election Systems & Software, Inc.(ES&S) Unity 3.0.1.0 voting system, which includes the iVotronic DRE, and the Hart InterCivic Polling Place System 6.0, which includes the eSlate DRE, both fail to meet numerous Colorado's requirements for certification of electronic voting systems, as prescribed in Colorado Election Code provisions and the Colorado Election Rules promulgated by the Secretary of State's office. Finally, it is my opinion that the continuous-roll, thermal-paper-based, voter-verified paper audit trail (VVPAT) systems currently certified by the Secretary of State violate Colorado's requirements that the electronic voting systems produce a permanent paper record, with manual audit capacity, of the voter's intent and that the voter's ballot remain secret.

I have generally considered two separate security issues: system integrity and voter privacy. Integrity refers to the ability of a voting system to resist malicious tampering as may occur during the administration of an election—specifically, whether the ultimate vote tally will accurately reflect the intent of every voter. Privacy refers to the ability of a voting system to prevent anyone from linking a particular vote to a particular voter, including the voter himself or herself, once a vote has been cast. A successful voting system must have all these security properties and other pragmatic properties, such as being robust against physical abuse and operator error, as well as being readily usable by voters and poll workers. When security mechanisms depend on end users to follow procedures correctly, then it is germane to consider those dependencies to be security issues, as well.

### B. Opinions Regarding the Colorado Secretary of State's Certification Procedures and Practices

Colorado's certification procedures and practices are insufficient to address security and reliability concerns. Colorado's counties cannot be expected to shoulder the burden themselves. The state's responsibility is to perform a competent review of the worthiness of voting equipment for use in its state.

The State of Texas, as a point of contrast, has a panel of six experts with a variety of different skills. Reports from these experts can be found on the Texas Secretary of State's web site (http://www.sos.state.tx.us/elections/laws/votingsystems.shtml). The experts express their own opinions on how each system may or may not be suitable. Some are clearly focused on statutory requirements while others are focused on whether the equipment is secure against threats.

It is my understanding that Mr. John Gardner serves the role as the sole examiner of voting systems for Colorado. I understand that he drafted the rules to which voting systems are held and he evaluated the extent to which the voting systems met the rules. From reading transcripts of Mr. Gardner's deposition as well as reading the "Voting Equipment Qualification Reports" for both Hart InterCivic and ES&S, I am convinced that Gardner lacks the necessary breadth and depth of experience to adequately carry out the duties to which he has been assigned. His lack of qualifications are obvious from

reading his deposition transcript as well as his background. In particular, for someone to be considered an "expert" in computer security, I would expect to see, at a minimum, significant training (either academic or industrial) as well as several years of industrial experience working with security issues. Based on Mr. Gardner's deposition transcript, I see he has no such experience. He does discuss having taken a Microsoft-certified evening course on administrating Windows NT 4.0 (deposition, day 1, page 19) but otherwise:

21

Q Do you have any technical training in computer security?
A Not to my knowledge, no.
Q Do you have any technical training in the evaluation of computer systems?
A I don't believe so.
Q Do you have any real-world experience in the security of computer systems?
A Yes.
Q And what's that?
A In my past previous jobs at the

22

architectural office, The Larson Group, I was the director of information services responsible for their entire system and software, which included some security.
For El Paso County, I was the information systems manager responsible for administration, security, operations of the applications that they use there.

Mr. Gardner's real world experience appears to have been in a systems administration capacity, at the Larson Group, and in a managerial capacity, for El Paso County. While systems administration does involve some security issues, such as ensuring users have reasonable passwords, anti-virus systems, and so on, it generally does not involve the in-depth analysis of systems for whether they are secure. Furthermore, without any formal or even informal training in computer science and software engineering, Mr. Gardner would not be able to ascertain whether a security claim, made in a vendor document, was truthful or was merely wishful thinking. In fact, Mr. Gardner repeatedly testified that he does not read nor analyze security information submitted by vendors or ITA reports. He merely checks the box that the information has been submitted in whatever form.

Later in this report, I will detail particular issues that I observed with both the Hart InterCivic and ES&S systems, which I would expect a competent examiner to be able to discover, but which Mr. Gardner did not discover. More generally, Mr. Gardner's reports are quite superficial in nature. While he does make helpful comments (e.g., pointing out

that voting equipment must be reset before each election in the Hart InterCivic certification, p. 6), he does not present any critical analysis of critical security features. I am particularly stunned by reading the appendices which present a list of requirements, annotated with "P" (pass) or "F" (fail) with little or no elaboration beyond this point. While such minimal effort may be sufficient to determine that a particular document has been submitted by a vendor, it requires additional effort to determine if the documents in question actually say anything interesting. These appendices also claim to be the test log of Mr. Gardner's testing of the voting systems. Again, little or no elaboration appears beyond the "P" or "F" marks. This makes his testing insufficient for any independent observer to be able to reproduce his results and does not meet the requirements of the Colorado Rules for Election Systems (see., e.g., rule 45.6.2.2.3). Mr. Gardner also does not follow and apply the failure criteria of rule 45.6.3 (notably, "Voting systems shall successfully complete all of the requirements in this rule, and any additional testing that is deemed necessary by the SOS.").

Starting from a young age, children are taught in science and mathematics classes to "show their work." A fundamental tenet of science is that a result should be reproducible and that a research report must present enough information for an independent observer to replicate the same result. This level of rigor is equally critical for the analysis and certification of voting systems. A mere "P" plus illegible notes in the margins is stunningly inadequate, yet that is all that Mr. Gardner did (so far as we can observe) during his examinations. None of Mr. Gardner's procedures follow proper testing methodology, as would be expected in any other scientific or technical endeavor. A proper test should have objective criteria for what passes and fails the test, and the tester would be required to document all the evidence and procedures followed in gathering the data necessary to evaluate the test criteria. Instead, Mr. Gardner failed to do this for all of his tests (see, e.g., Gardner Deposition, Day 2):

347

Q … And this would be the same for each and every one of the four subject DRE systems?
A Yes, the test is the same.
Q And this would be the same for the Sequoia 5.0-A system?
A Yes.
Q This would be the same process that you would go through with your documentation of security and then functional testing?
A Yes, that is correct.
Q And we've -- the way I've described the functional testing that you do today, you agree with?
A Yes, I believe so.

Furthermore, as I will describe later, there are security-critical documents referenced in the materials submitted by both Hart InterCivic and ES&S which were not included in the materials they submitted to Colorado. Had Mr. Gardner read the submitted documents, he would have recognized that security critical content was missing and would have requested it. Instead, Mr. Gardner appears willing to allow a reference to an unseen document as being sufficient proof for a system being secure. See, for example, his deposition transcript (day 1, page 138):

Q So whatever a voting-system provider submits is good enough, correct?
A That is all that's requested by the rule.
Q Okay. And all that you do to determine that it's good enough is you look and see that it's present in the documentation, correct?
A Yes.
Q You don't look -- you don't analyze that documentation to see if that is -- a robust minimum standard has been met?
A Aside from the functional tests that we do, which we discussed earlier.

Mr. Gardner admits that he does not read the documents, but instead relies on federal certification (i.e., ITA testing), whether or not that ITA testing is sufficient to guarantee any compliance with Colorado statutes or rules. As I will discuss later, I believe neither Hart InterCivic nor ES&S's voting systems appear to be in compliance with Colorado statutes and rules.

For Colorado to determine if its voting systems are meaningfully secure, the state would need to both write more stringent rules as well as performing a more serious analysis. Colorado would recognize the insufficiency of the present ITA reports and would commission professional security analysts to conduct independent studies of its voting equipment. Where such studies have been performed, a variety of additional security failures have been brought to light, allowing states to require improvements to their voting systems. A handful of these studies are performed by independent experts based on public documents (such as the work of Dr. Harri Hursti or my own work), while most are commissioned by states. Maryland and Ohio hired independent contractors (SAIC and RABA, by Maryland, and InfoSentry and CompuWare, by Ohio, respectively). California hired two academic security experts (David Wagner, from U.C. Berkeley and Matt Bishop from U.C. Davis) along with an expert from Lawrence Livermore National Labs (David Jefferson). In several of these cases, notably the RABA and California reports, the examiners were given carte blanche to examine anything and everything with an eye toward election security. This form of "red team" or "tiger team" exercise is widely regarded as an important means of identifying security vulnerabilities. Further studies might consider the development practices of the companies, as poor development

practices are largely guaranteed to produce faulty products. Had Mr. Gardner, in his capacity as the drafter of Colorado's rules for voting equipment, been a security expert, he would have drafted far more stringent requirements as well as more stringent evaluation methods than those that he performed, himself. Remarkably, while the Colorado legislature requires the Secretary of State to promulgate minimum standards for election security (C.R.S. 1-5-616(1)(a)-(g)), the relevant rules drafted by Mr. Gardner (rule 45.5.2.6) merely require that the vendor submit documents claiming to discuss security rather than actually requiring any review of those documents, much less the voting systems themselves. In my opinion, the Secretary of State's rules do not satisfy the legislature's requirements for "minimum standards for electronic and electromechanical voting systems." Curiously, even though Mr. Gardner authored the rules, he claims he has no idea where he came up rule 45.5.2.6 (see, e.g., Gardner Deposition, Day 1):

90

Q And what was the source of the security requirements?
A I don't -- I don't recall where they'd come from. The issue is: We have this document, which was Drew's document.
I also have some information from California, some information from Georgia, some information from New York; the 2002 voting-system standards, the draft of the 2005 voluntary voting-system standards, and a variety of guidance and direction as to which way to go.
So did those come from the voting-system standards? Did they come from California?

91

Did they come from a Texas document? Did they come from Drew's document? I'm not sure.
Q You don't know. And this was the first time you'd ever tried to do something like this, as well, right?
A Yes. Sure.

Finally, I will note that it is an accepted practice in security evaluation for the evaluators to make conservative statements with regard to a systems' security. A security evaluation will always speak toward a *particular* configuration with a *particular* software version. Any changes in the software or the system configuration could invalidate the assumptions behind the evaluation. Mr. Gardner appears to be cavalier in his approach toward this concern. For Hart InterCivic, he only has "preliminary" evaluations, yet he certified the system. For ES&S, he only had evaluations of Unity 3.0.0.0 while he certified Unity 3.0.1.0. Certainly, it's valuable to get newer software with its bug fixes and whatnot into the hands of the counties who will be using it, but there needs to be a process to ensure

that the changes introduced truly are improvements over the status quo. This is exacerbated by the voting system vendors' need to support varying requirements in each of the 50 states. For example, Texas requires DREs to have a "straight ticket" voting feature while California forbids any such feature. As such, every "point release" of a vendor's software must be carefully analyzed to ensure that it meets the requirements that will vary from state to state. Mr. Gardner has failed to do this.

### C. Opinions Regarding the Secretary's Designation of "Security Information" to Shield Documents Against Disclosure

In the course of my investigation for this case, I was required to fly to Denver, twice, to read documents that were considered "Confidential" and/or "Attorney's Eyes Only" which were only available to be read in a conference room in the office of the Attorney General. We were forbidden from making photocopies or even from having cell phones or computers. Initially, large security-critical aspects of the documents were redacted, in their entirety, by the Attorney General's office. In my opinion, these redactions and the extreme measures required to handle the documents was entirely unnecessary given their contents. I have served as an expert witness in several patent and trade secret cases. At one point, I even had access to source code considered by Microsoft to be exceptionally sensitive to their business. In all of these cases, the protective order in the case was sufficient to allow me to handle documents in my home and office without attorneys for either side being concerned that confidentiality would be breached. In this specific case, the need to have further secrecy was unwarranted. If every single document I read were to be made available to the public, the only damage would be to the reputations of the vendors (for the poor quality of their systems) and to the independent testing authorities (for the poor quality of their analyses).

The judge's original order, to protect "source code" is sensible, insofar as source code is commonly considered to be proprietary to a given vendor and its disclosure would leak trade secrets considered by a vendor to be valuable business property. (Whether trade secrecy is in any way appropriate in a voting system is a separate debate.) However, *there was no source code, as such, anywhere in any document that I had the opportunity to read.* Instead, I saw documentation that closely related to the source code, describing the various changes made and bugs repaired. I saw the names of files and the layout of data structures for data that would be considered public information (e.g., data structures for how votes are written to memory cards). I saw brief excerpts from source code, but nothing substantial or illuminating.

While I never saw any proper source code, I was still able to find a variety of issues which could well lead to critical security flaws. *This does not mean that these documents' secrecy is an impediment to the exploitation of these security flaws.* This is a debate that goes back to the original locksmiths, wondering whether it would be appropriate to discuss lock design and lock picking in public. The assumption, then as now, is that "rogues" will always know how the locks (or voting systems) work. They're already having this discussion, so the "good guys" might as well be having the same discussion to hopefully stay ahead of the rogues. Today, this is widely considered a

fundamental principle in computer security: *a system should be secure, even if the adversary knows everything there is to know about how the system works.*

As such, I conclude that no useful purpose was served by the extraordinary protection granted to the "confidential" and "attorney's eyes only" documents. I further conclude that no useful purpose is served by these documents being anything other than made fully available to the public.

### D. Software Quality, Reliability, and Security

Generally speaking, software quality is fundamental to the enterprise of electronic voting and tallying. Where software is used, it could fail, and software failures could potentially compromise the results of election. Broadly speaking, two strategies may be implemented to address this concern. Software may be subject to a rigorous *process*, throughout its development and certification, to methodically remove bugs and engineer a stronger product. Furthermore, the risks may be *mitigated* by having redundant and independent means of achieving the proper result. Voter-verified paper audit trails, as discussed in detail below, represent an important mitigation strategy, but that strategy depends on voter and poll-worker vigilance. Ideally, a voting system would be robust even when human vigilance is lacking.

Software security is really a special case of software quality. If older, lower-quality development tools and programming languages are used, the software will have more defects. Likewise, if the software design process, performed by the software developers, is unprincipled or chaotic, then bugs will not be found and critical design flaws may be "baked into" the system.

Vendors presently submitting their equipment for certification in Colorado have been presenting to the Secretary of State independent testing authority (ITA) reports that are supposed to test the voting system for compliance with the 2002 Federal Election Commission (FEC) voting guidelines. Where those guidelines speak to software engineering processes, they require largely cosmetic features, such as reasonable software commenting standards. They do not require deeper design principles. They do not require quality assurance processes or internal design reviews. They say nothing about security threat analysis, in the design, or penetration/red team analysis, of the finished product. The net result is that voting system software with strikingly obvious flaws can sail through the certification processes in Colorado and other states if those states do not require more than the submission of ITA reports.

The most widely studied example of this is Diebold's AccuVote-TS and TSx systems. In 2003, Diebold accidentally left their source code on a public web server, which was discovered and widely copied. I co-authored a study of this source code (with Tadayoshi Kohno, Adam Stubblefield, and Aviel D. Rubin, and published in *IEEE Security & Privacy* (May 2004)) in which we discovered and described a variety of problems. For example, every Diebold DRE ever manufactured used the same cryptographic key. The use of a common cryptographic key means that any cryptography done with that key is

meaningless. Any intercepted communication could be easily decrypted, modified, and retransmitted. Likewise, we found a subtle attack that would allow voters, in some cases, to cast multiple votes. Subsequent to our own study, a variety of follow-on studies have been commissioned by other states, including Maryland, Ohio, and California. Our original findings have all been confirmed, and other, even more significant attacks have been discovered, such as those recently identified by Dr. Harri Hursti.

While this certainly speaks poorly for Diebold, it speaks even more strongly about weaknesses in the ITAs, which are required by most states, including Colorado, to "certify" voting systems prior to state approval. Glaring, obvious security holes in the Diebold system repeatedly escaped ITA attention. Given that this is true for Diebold, it raises questions about the ITAs' ability to discover problems with other voting system vendors.

In the course of my investigation for this case, I had the opportunity to read ITA reports as well as portions of the "technical documents package" (TDP) submitted by the vendors to the ITAs and Colorado. Below I discuss my findings concerning two DRE voting systems certified in Colorado: the Hart InterCivic "Polling Place 6.0 System" (including the eSlate and eScan systems) and the ES&S Unity 3.0.1.0 / iVotronic 9.0.

### 1. Hart InterCivic Polling Place 6.0 System

Colorado received relatively little ITA and technical documentation from Hart InterCivic regarding the Polling Place 6.0 System. While the ES&S technical and ITA documents occupied two large boxes, the stack of Hart InterCivic documents was not even six inches tall. The Hart InterCivic ITA reports were the "Software Qualification Test Report for Hart System 6.0" (1/13/06, produced by Ciber) and the "Hardware Qualification Testing of the Polling Place System 6.0" (1/11/06, produced by Wyle). Both documents were prominently stamped "Preliminary." While I am not fully aware of the process through which a "Preliminary" document becomes "Final" (the vendor-to-ITA conversation is generally protected by non-disclosure agreements), the "preliminary" nature of the documents suggests that they should not be relied upon for making a final determination as to the fitness of a particular voting system. The failure of the Secretary to obtain final ITA reports from Hart InterCivic demonstrates that the Secretary did not even enforce her documentation requirements enumerated in Rule 45, let alone evaluate documents for substantive compliance with Colorado law. Even a cursory review of the preliminary ITA reports would have revealed many gaps in Hart InterCivic's certification application and the ITAs' failure to properly evaluate and certify the system as compliant with the 2002 VSS, including the following issues:

The Wyle report on Hart InterCivic's hardware explicitly states that it does not consider source code security:

The Wyle report contains a grid, breaking down the 2002 VSS standards and giving test results for each section. All sections with any security relevance are either listed as "not tested" or "not applicable." For example, all of the

section 5 ("telecommunications") functional requirements were not tested, despite the fact that Hart InterCivic's system allows for precinct-level voting information to be accumulated at regional processing centers (using the "Rally" software package) then transmitted to a central facility (for ultimate processing with the "Tally" software package). That transmission necessarily requires telecommunications of some sort. Similarly, necessary security features such as "6.4.2 protection against malicious code" were not tested at all. Likewise, all the security features of "6.5 Telecommunications and Data Transmission" and "6.6 Security for Transmission of Official Data over Public Communications Networks" are listed as "not applicable," even though they clearly are. Perhaps Wyle conducted the applicable testing before it issued a final report on the hardware, but Colorado did not obtain a copy of the final report to determine whether these gaps still existed in the final ITA report.

The Ciber report on Hart InterCivic's software is no improvement over the Wyle report. The only source code review, such as it is, appears in Appendix B – with only three pages of meaningful content plus a long and irrelevant list of the source code filenames that were submitted to Ciber. Even among those three pages, none of the comments showed any evidence of significant security analysis. Instead, we see concerns such as "4.2.7a3 Module header needs comments for inputs and outputs" or "4.2.7a6 Module header needs revision history." If Ciber were to have analyzed any of the security mechanisms used by the Hart InterCivic system, one would expect to see commentary describing how it works, what vulnerabilities were found, and how they should be addressed. Even if the voting system were completely and utterly secure (and few software systems are), I would expect to see analysis describing the extent to which Ciber attempted to break the system's security and why Ciber failed. *The Ciber report contains absolutely no evidence that they performed a meaningful security analysis of the Hart InterCivic system.* (See my earlier comments about "showing your work.") Based on my reading of Mr. Gardner's deposition testimony, Mr. Gardner did not even read the Ciber report for substance, and to the extent he did, he did not appreciate the extent to which it lacks any meaningful security analysis.

Beyond this, the only documents available to the state of Colorado for analyzing the integrity of the Hart InterCivic system were those submitted by Hart itself. That list of documents is quite thin. The following documents were available in the Attorney General's conference room, marked "confidential" and/or "attorney's eyes only":

- eCM (eSlate Cryptographic Module) Manager Operations Manual (Rev 11-60B, 2005);
- BallotNow Change Document (Rev 32-60A, 9/2/2005);
- PVS (Precinct Voting System) Change Document (Rev 40-60A, 11/23/05);
- eCM Manager Change Document (Rev 11-60A, 9/28/2005);
- BOSS Change Document (Rev 42-60A, 10/17/2005);
- eScan Change Document (Rev 11-30A, 12/7/2003);
- Rally Change Document (Rev 22-60A, 10/10/2005); and
- Tally Change Document (Rev 42-60A, 10/12/2005).

Several other documents on Hart InterCivic systems were also available to me outside of the aforementioned conference room, but they were only operations manuals or user guides. There was no meaningful security discussion in these other documents.

The eCM is interesting from a security perspective because it uses a hardware token as an alternative to traditional user names and passwords. Unfortunately, Colorado only received the user manual, not any discussion of how it works, much less any analysis of how hard it might be to make an unauthorized copy. The manual does point out, however:

p. 33.) Poor grammar aside, this implies that a copying process exists, which could potentially undermine whatever security is provided by using the eCMs. This is a red flag for any security analysis, demanding further investigation to determine how the eCM copying process works. No such information or analysis appears in the Hart documents, in the ITA reports, or anywhere in any of Colorado's certification documents.

Apparently, the State of Texas requested further information on the functioning of the eCM. A letter was written by Hart InterCivic Vice President Neil McClure which purported to describe how eCM works:

> The USB key is used to digitally sign data whenever the data is moved from one system component to another. … When the data is within a system component, it is secured by the system authentication requirements, the Principle of Least Privilege, Segregation of Duties, and Role-Based Privileges. … Please refer to the Symantec white paper "Securing the eSlate Electronic Voting System Application Security Implementation" (attached) for further details of the comprehensive security surrounding the Hart Voting System.

(Letter from Neil McClure to Ann McGeehan, Texas's Director of Elections, July 2005, available at http://www.sos.state.tx.us/elections/forms/sysexam/0505hartletter.pdf.)

Mr. McClure uses a variety of terms that are used when engineering secure software systems, such as the Principle of Least Privilege, but says nothing about how well the Hart system satisfies this principle or any other design principle. The referenced Symantec paper is also available on the Texas web site. The document largely describes a Symantec security-conscious development process that Hart has apparently now adopted. The document contains no critical analysis of the security of the present product. For example, a security feature intended to prevent software tampering is described:

> **Continuous DRE integrity checks** – the eSlate and JBC components run continuous background monitoring to ensure the integrity of the executable

> firmware. Firmware is stored internal to the device in nonvolatile memory along with a verification table that provides a cyclic redundancy check (CRC) code for each of several code sections. When the embedded, realtime operating system begins code execution, a system task performs a CRC calculation of each code section. The system is halted with a failure message if the calculated CRC does not match the expected value from the verification table. This verification operation is performed continuously while the system is active and provides protection against hardware failures and attempts to corrupt the eSlate or JBC application.
>
> **Code verification** – The firmware resident in the eSlate components is audited against unauthorized changes by SERVO, both before and after the election. A cryptographically secure digital hash provides verification that the eSlate firmware is identical to the certified version on file with the National Software Reference Library (NSRL) which is managed by the National Institute of Standards and Technology (NIST). This provides an additional technical protection against attempts to modify election software on voter terminals.

(Brad Arkin, "Securing the eSlate Electronic Voting System: Application Security Implementation," May 2005, p. 11, available at http://www.sos.state.tx.us/elections/forms/sysexam/hart_symantec_security.pdf.)

Arkin's analysis raises far more questions than it answers. How exactly is the firmware audited against unauthorized changes? What protections are in place when the firmware itself is upgraded? How hard would software tampering be to achieve in practice? These questions are entirely unanswered yet are fundamental to the question of security for the voting system! Even if somebody from the Colorado Secretary of State's office had read this document (despite substantial evidence to the contrary), a competent security analyst should have demanded a far more detailed consideration of this and of other important security issues.

Of the remaining documents submitted to the Colorado Secretary of State, the change documents only discuss changes to the various modules of the Hart voting system. They make reference to matching "Requirements Specification" and "Functional Specification" documents for each module, as well as some "Security Specifications" documents, none of which were provided to Colorado. Instead, these documents tend to say things like "Changes to fix defects found in testing" or even "Corrected per Ciber review." This is not only completely devoid of any useful information, but it displays the vendor's contempt for the entire certification process. One would presume that a "change document" would provide meaningful details about what changed from one version to another. What problem did Ciber find? How was the problem fixed? No useful information was provided to Colorado at all.

As far as I can observe, Colorado certified the Hart voting system based on two "preliminary" ITA reports and absolutely no meaningful vendor documents. This

appears to be a clear violation of the Colorado Election Code and Election Rules. The relevant Election Rule, which Mr. Gardner himself authored, requires:

> This documentation shall include information that defines the voting system design, method of operation, and related resources. It shall also include a system overview and documentation of the voting system's functionality, accessibility, hardware, software, security, test and verification specifications, operations procedures, maintenance procedures, and personnel deployment and training requirements. In addition, the documentation submitted shall include the voting system provider's configuration management plan and quality assurance program. (45.4.3)
>
> In addition …, the voting system provider shall provide the following documents:
>
> - Standard Issue Users/Operator Manual
> - System Administrator's Manual
> - Training Manual (and materials)
> - Systems Programming and Diagnostics Manuals (45.5.2.4.1)
>
> All ITA qualification reports that are material to the determination that a voting system may be certified shall be evaluated to determine if the test procedures, records of testing, and reporting of results meet the requirements of this rule. (45.5.2.4.2)

The necessary Hart InterCivic documents were simply never submitted to the Colorado Secretary of State. As such, the Hart InterCivic system should never have been certified for use in the State of Colorado. Had those documents been submitted, then other important security concerns would have become apparent to a skilled security analyst, who would then be able to identify other violations of Colorado statutes and rules.

### 2. ES&S Unity System 3.0.1.0

ES&S submitted a significant volume of paper (two large boxes) to the Colorado Secretary of State. I will begin my analysis by considering the ITA reports and then I will consider the ES&S internal documents.

**ITA Reports on ES&S Unity System**

There were, in total, five Wyle reports, one Ciber report, and one Systest report.

Although Mr. Gardner testified that ES&S's Unity System 3.0.1.0 was certified (Gardner Dep. at 164:1-23), and not the Unity System 3.0, there is no evidence that the State of Colorado ever received final ITA reports for all the components of the Unity System version 3.0.1.0. As I discussed above, a security analyst must consider the actual system being certified to ensure that the changes between the two systems do not impact the certification. Mr. Gardner does not appear to have done this.

Furthermore, even Mr. Gardner's examination shows that the ES&S system failed several of the tests and therefore should have failed the certification according to the mandatory aspects of rule 45. Mr. Gardner's deposition transcript also indicates he was under some political pressure from Mesa County to certify the system (see, e.g., Gardner Deposition, Day 1):

225

Q Okay. And then when you and Secretary Dennis met on the phone with Sheila (sic) Ward when you had the meeting about the complications and the certification review, there was political pressure from Mesa County to grant the certification; isn't that right?

A Are you referring to Janice Ward?

226

Q Janice Ward, yes.

A Okay.

MR. KNAIZER: I'd just object to the form of the question.

But go ahead and answer.

A That was in -- at the end of the month?

Q (BY MR. HULTIN) Yeah.

A Yes. Sure. Yes, there was some pressure.

Q She said, "Do it"?

A Essentially.

Q And the Secretary did it?

A With some conditions, yes.

I first considered Wyle's "Hardware Qualification Testing of the ES&S Model 650 Central Ballot Counter, Firmware Release 2.0.1.0" (January 2005). The source code review was entirely a superficial consideration of each source code file, pointing out issues such as problems with variable names or code commenting style. There was no discussion, whatsoever, of higher-level design issues. This report did point out some evidence of a poor software engineering process:

I will revisit this issue below.

Wyle's "Hardware Qualification of the ES&S iVotronic (Firmware 9.0.0)" (November 2004) was similarly superficial in its source code review. For example,

As before, there is no deeper analysis of whether the software design is actually secure.

Wyle's "Hardware Qualification Testing of the ES&S Model 100 Precinct Counter" (February 2005) was more critical, with a large number of comments describing lines of code where

A lack of bounds checking is widely understood to make software vulnerable to crashing as well as to external attack, so these concerns are quite serious. Similarly, there are comments such as

Even with the redaction (at most a few words, probably the name of a function within the C program), it's quite clear that the software engineering *process*, as a whole, is quite suspect if it would allow such blatant problems to go out the door, with or without an ITA to hopefully catch them. This report does indicate that Wyle tentatively rejected one software revision (5.0.0R):

As with other Wyle reports, there is no evidence of any deeper analysis of whether the software design is actually secure.

Wyle's "Change Release Report of the ES&S Model 650 (Firmware 1.2.0.0)" (February 2004) has a variety of minor comments, but does point out that

Again, we see Wyle qualifying its statement. As with other Wyle reports, there is no evidence of any deeper analysis of whether the software design is actually secure.

Wyle's "Change Release Report of the ES&S iVotronic (Firmware 8.0.0.0)" (February 2004), while lacking in depth as with other Wyle reports, still points out a critical flaw in ES&S's software development processes. This report details a back-and-forth exchange between Wyle and ES&S concerning a variety of different iVotronic firmware releases:

8.0.0.0ZM: received at an unspecified date
8.0.0.0ZZD: received July 16, 2003
8.0.0.0ZZH: received July 25, 2003
8.0.0.0ZZI: received July 29, 2003
8.0.0.0ZZJ: received August 15, 2003
8.0.0.0ZZL: received September 10, 2003
8.0.0.0ZZM: received September 29, 2003

It required five round-trips between ES&S and Wyle before Wyle was willing to consider the ES&S software (version 'ZZJ) to be in compliance with the 2002 FEC guidelines. The Wyle reviewers, looking at the 'ZZH code, were clearly exasperated with ES&S's performance:

A similar issue is noted in James Sneeringer's report to the Texas Secretary of State:

> ES&S presented us with two sets of software change logs, one with their initial submission and another when they presented additional equipment to be examined. The changes listed appear to be completely different, even though the logs were for the same product and in some cases covered the same version range and the same data range. This examiner attempted to match the changes listed in the two reports, on the assumption that they were the same changes but were reported in a different order and worded slightly differently, but found almost no duplication between the reports. ES&S told us that the newer reports are the accurate ones, but they offered no satisfactory explanation of where the other reports came from. At the exam, they submitted a third set of reports that were consistent with the second set, the only differences being some entries for additional changes made since the second set of reports.
>
> …
>
> **Recommendation**: Certification should be denied unless there is a satisfactory explanation. A development process that produces reports with contradictory information is not acceptable, and the integrity of the examination process relies on examiners receiving correct information from vendors.

(James Sneeringer, Ph.D, "Voting System Examination: Election Systems & Software (ES&S)," June 2004, available at http://www.sos.state.tx.us/elections/laws/may2004.shtml.)

The rapid back-and-forth between ES&S and Wyle, and the commentary of the Wyle reviewer, are directly indicative of an ad hoc software development and testing process within ES&S. Sneeringer's observations indicate that this was not an isolated incident.

A poor software engineering process is virtually guaranteed to yield low quality code, leading directly to a higher likelihood of crashing and of having security vulnerabilities. I agree with Sneeringer's conclusion that this raises significant concerns about the vendor's ability to deliver systems of the necessary quality to run elections.

Ciber's "Software Qualification Test Report for Unity 2.5" (October 2004) is superficial, as described above for their Hart InterCivic report. Interestingly, their evaluation claims that

This statement is entirely false! COBOL, in particular, which is used for a large part of ES&S's code base, is a programming language that predates the very idea of object-oriented programming. Even newer languages, like Java, which are indeed built to *facilitate* object-oriented programming, have no mechanisms whatsoever to *enforce* good design or programming methodology. Enforcement comes from having skilled programmers operating within a rigorous process of internal design and code reviews. A statement like Ciber's directly indicates that Ciber has absolutely no idea what it's talking about.

Finally, Systest's "Unity 3.0 Voting System, Hardware & Software ITA Qualification Report" (October 2005), considers the ES&S system that is one version earlier than the 3.0.1.0 version currently certified in Colorado. (As noted above, there is no evidence that ES&S produced to Colorado a final ITA report for Unity 3.0.1.0.) The source code review, as with reviews from other vendors, has no indication that anything beyond superficial issues was considered. The source code review summary (Systest Rep. pp. 25-29) indicates no analysis more sophisticated than pointing out that several functions have more than 240 lines of code within them. Appendix B (pp. 60-79), intended to offer more details, is simply a giant table that breaks down the requirements of the 2002 VSS guidelines, with an integer count of how many source code files satisfy each element of the standard. Absolutely no details are presented about how the analyses were performed, what was considered, and so forth.

When a standard requires something simple, such as stating that all variables must have reasonable names, comments describing their functions, and must have their values properly initialized, there is no need for any detailed analysis. However, when a standard speaks of security, reliability, secrecy, and other related topics, the burden on the testing authority is much stronger. Absent a detailed analysis that describes attempted attacks, design features, configuration issues, and so forth, there is no reason to believe that any of these ITAs performed at a level commensurate with Colorado's requirements concerning security, privacy, durability, and reliability.

**ES&S's Internal Documents**

I will note that, despite the large volume of documents submitted by ES&S, several important and widely cross-referenced documents are missing from Colorado's files.

Most notably, several documents refer to a document entitled "Election Security Concepts and Consideration, version 1.2, 8/26/2004." Likewise, there were numerous references to the "ES&S Coding Standards & Development Practices," which is also germane to security analysis of the voting system. These documents, while clearly relevant to Colorado's examination, were absent from the materials reviewed by the State and produced in discovery to Plaintiffs' attorneys and experts. Even a cursory study of the submitted documents by the Secretary of State's office, with an educated eye toward security issues, would have discovered these references. By their absence, I can conclude that no such study was performed by anyone in the Colorado Secretary of State's office. Despite this, I will consider the documents that were available and describe what security issues and questions they reveal.

I begin with the "ES&S Software Specification / Hardware Programming Manager, version 5.2.3.0" (January 2006). This massive, 910-page document contains a variety of low-level details, including file formats, for the Hardware Programming Manager package (normally used to set up ballot styles, precinct definitions, and so forth). Whenever security issues are raised, this document refers the reader to the "ES&S Coding Standards & Development Practices," which is not among the ES&S-submitted materials. Probably the most interesting details available in this document are, for most source code files, a listing of all the bugs that had been addressed with respect to that file. While this ES&S document represents a significant improvement over the Hart filings for revealing internal details of the vendor's operations, the revealed details are not flattering. For example, "08-13-03 (BUG0367) Write-in options on Eagle Specification screen do not function properly. When you check 'process write-ins', it ignores it, and when you uncleck 'process write-ins', it accepts it. It seems to be doing the opposite of what it should. Changed verbiage on screen to read 'Write-ins Ignored.'" (page 171). Rather than repairing the problem, it appears that they simply papered over the problem, hoping that nobody would notice it. This evidence further supports my contention that ES&S lacks a disciplined software development process.

Further evidence of ES&S's poor development process appears in the "ES&S Software Specification, iVotronic DRE Touch Screen / ADA Voting System, version 9.0.0.0" (July 2004). This refers to ES&S's most recent software for the iVotronic DRE system. I was particularly taken aback by this section:

Amazingly, there are no security books of any sort on ES&S's list, and that's not for any lack of publications on the topic. One would imagine ES&S would at least consider blockbuster titles like Microsoft's "Writing Solid Code" (originally published in 1993, now available in a second edition, published in 2002), Ross Anderson's "Security Engineering" (originally published in 2001 and widely used as a college textbook), or Bruce Schneier's "Secrets and Lies: Digital Security in a Networked World" (published in 2000; Scheneier was the inventor of the Blowfish encryption algorithm used by ES&S).

The ES&S developers' apparent lack of competence extends well beyond their lack of an understanding of computer security. One striking example:

Assemblers are part of the standard toolchain used when developing software. An assembler only ensures that the resulting binary program will execute on the target computer. Assemblers make no guarantees that the resulting file is meaningfully correct or uncorrupted. Likewise, this "conversion utility" could do anything or nothing with respect to data corruption. No details are provided.

The bulk of the "software specification" document is a series of pages, one per source code file, that purport to explain the purpose of each of those files. Here's one example:

With the exception of the initial two sentences, everything else here was repeated for each and every file. The "logic used" is tautological, at best, and certainly lacking in meaningful detail. The "constraints, limits, or unusual features" section should be documenting things that other developers or auditors might find notable about this particular source code file. Instead, this standard boilerplate is used throughout the document. As a result, the only meaningful information is the initial two sentences. The Federal requirement for documents, such as this, is intended to enforce a discipline on the engineering process. Meaningful processes should produce meaningful documentation of how the system works. This particular document makes a mockery of disciplined software engineering.

**Encryption**. While reading the ES&S Software Specification for the Hardware Programming Manager, I came across this:

There is no sensible reason for encrypting a ballot file. Digital signatures, as used by Hart InterCivic, can be used to detect tampering. Encryption only serves to make it difficult for independent tools to read critical voting data, while offering no protection against tampering. After reading this, I endeavored to learn more about how ES&S does their encryption. There are numerous references to the Blowfish cipher (a symmetric-keyed encryption system designed by Bruce Schneier, considered obsolete after NIST adopted the advanced encryption standard (AES) in November 2001). Blowfish is a traditional encryption algorithm, providing neither digital signatures nor any sort of key management architecture. (Key management is widely considered to be the most difficult aspect of building a cryptographic system.)

This led me to look for further details on how ES&S actually implemented its encryption. The ES&S Software Specification for the iVotronic contains "Appendix C: iVotronic File

Layouts," which describes how ballot information is written out to memory cards, which may then be transported to the elections administrator for tallying. One striking element was the "Configuration" section, meant to describe the various settings of the machine. Several items caught my attention:

This says several interesting things. Most interestingly, the Blowfish encryption key is stored alongside the very data it is meant to protect – a fundamental security error. Furthermore, an insecure 16-bit CRC is used for data integrity protection, rather than a more robust digital signature technique. This system provides absolutely no meaningful security. It demonstrates a complete lack of understanding for how cryptographic primitives are meant to be used. In addition to offering no protection, it raises the specter of corruption of the encryption system, resulting in unreadable audit data.

From this I can only conclude that one of ES&S's customers required them to add "encryption," but because neither the customer nor ES&S had any idea what that entailed, an unskilled developer cobbled something together to meet this requirement. *This is a glaring design flaw. Any security-aware auditor, reading this, would immediately flag it as unacceptable.* As a direct result, election results and audit data are unnecessarily vulnerable to tampering. This is a clear violation of Colorado election rules and should have resulted in the disqualification of the ES&S system. For example:

> All electronic transmissions across public networks shall be secured to the level and using the technologies prescribed in the State of Colorado's "Minimum IT Architecture Standards" as adopted by the Information Management Commission at the time of certification. The voting system provider shall provide documentation describing in detail the steps and methods used for those electronic transmissions. This documentation will describe, at a minimum, the methods by which authentication, confidentiality, integrity, and availability of the transmission and verification of electronically transmitted information will be performed. (Colorado Election Rule 45.5.2.7.2)

This rule clearly requires confidentiality and integrity be maintained, but ES&S's design fails to maintain either.

ES&S did produce a document titled "ES&S Secure Voting System Overview for Unity, version 3.0.1.0" (December 2005). This document contains "high-level system descriptions required to fulfill FEC requirements" and is largely filled with illegible block diagrams and flow charts. While there is a list of security features, there is no vulnerability analysis or any other attempt to convince the reader that the security features are properly implemented and address the threats the system may face. This is particularly evident in the "System Security Specification" (starting at page 171). Whenever details might have been described, instead we see this:

Assuming the Secretary has produced all responsive documents to Plaintiffs, the referenced "election security" document was never provided to Colorado as it should have been.

### E. VVPAT Systems Certified for Use in Colorado Elections

Colorado statutes now require any electronic voting system to "produce[] the records necessary to audit the operation of the electronic or electromechanical voting system, including a permanent paper record with a manual audit capacity." C.R.S. § 1-5-615(1)(p). Further, "[t]he permanent paper record produced by the electronic or electromechanical voting system shall be available as an official record for any recount conducted for any election in which the system was used." C.R.S. § 1-5-615(2). Also, any electronic voting system acquired after June 6, 2005, must "be capable of producing a voter-verified paper record of each elector's vote." C.R.S. § 1-5-801(1). Computer-based DRE systems, absent any printer that produces the requisite permanent paper record of individual voters' votes, would not satisfy these statutory requirements. All the major vendors now offer printers that may be attached to DRE systems, with the intent of satisfying these auditable paper trial requirements.

VVPATs have the *potential* to satisfy several properties that are important for voting systems. Most notably, a computer cannot modify or "un-print" something once it has been printed. A VVPAT printout serves as a *commitment* to a particular expression of a voter's intent. If, thereafter, the electronic records are tampered, corrupted, or simply lost, the voter's original intent can be recovered by examining the paper trail, with the confidence that the voter personally saw, read, and approved of that piece of paper. VVPATs also increase the *transparency* of an election. Humans cannot observe the actions of software within a machine, but they can observe the printing and handing of paper. Increasing transparency serves to increase confidence that, should there be a problem, it can be detected and corrected.

Most DRE vendors, including the four presently considered in Colorado, have adopted VVPAT printers that use a continuous roll of thermal paper, which is held behind a glass

screen or window. Because a comparable mechanism is used, a comparable analysis can be performed. My analysis and opinions regarding the VVPATs used in Colorado are as follows:

- The use of thermal paper—the same kind of paper used by many receipt printers and that was commonly used by old fax machines—is an inappropriate choice given the VVPAT and permanent-record requirements set out in Colorado law. C.S.R. §§ 1-5-615, 1-5-802(3), 1-7-802 (ballots must be preserved for at least 25 months after election). In addition to the Colorado law specifically requires that "[a]ll paper, ink, and other materials used in public offices for the purpose of ***permanent records*** shall be of durable quality." C.R.S. § 24-80-106. Most problematic is the fact that thermal paper turns black when exposed to heat. Gas station receipts, for example, left on the windshield of a car will turn brown over time, even when they are not repeatedly handled. Moreover, thermal paper can smudge and degrade if it is repeatedly handled by multiple persons, such as would happen in an actual recount situation. These degradation issues affect ballots printed on thermal paper. This raises important concerns about document handing and longevity, especially in the event of a manual recount, and violates Colorado's requirements that paper ballots be "permanent . . . with a manual audit capacity" (C.R.S. § 1-5-615(1)(p)) and "shall be sturdy, clean, and of sufficient durability" (Colorado Election Rules, 8 C.C.R. § 1505-1 (45.5.2.9.9)). Although procedures could be adopted to photocopy the thermal-paper ballots onto archival-quality paper, the process would be unnecessarily costly and cumbersome and would need to be automated to avoid the possibility of human error in the transcription process. A more efficient, cost-effective system would allow for VVPAT printing directly onto archival-quality paper in the first instance. Such printers, however, would need to be submitted and certified as part of a vendor's voting system.

- With a continuous spool of paper, which can be as long as 250 feet, the ballots are recorded in the order that they are cast by voters. Any observer who records or remembers the order in which voters arrived may later be able to violate voter privacy. This issue was discussed, in detail, in Colorado's *Complaint of Al Kolwicz Concerning Hart/InterCivic eSlate Voting Equipment*. The Secretary's arguments against this attack are unpersuasive. So long as a record exists with the votes in the order in which they were cast, that record may at some point be used to compromise the voter's privacy. Hart InterCivic Vice President Neil McClure's response (SOS-HAVA-01-06-0001, Exhibit 3) is particularly troubling on this point. McClure posits that an attacker "can only ***claim*** to know how somebody voted because there is no proof." This is false. An attacker with information about the order in which voters appeared can read the individual votes, in order, from the logs. While this may not be sufficient proof for an independent observer, it would certainly be sufficient proof for the attacker. Historically, anonymous voting was instituted to defeat problems with voter bribery and coercion. If an attacker can convince him or herself of how voters voted, or can even make a credible threat of such an attack on the voter's privacy,

then voter intimidation or bribery is not only possible, but historically has been the probable result of voting systems that do not ensure voter privacy and secrecy of ballots. In fact, the Commonwealth of Pennsylvania was so concerned over this threat that Pennsylvania banned the use of these kinds of VVPAT printers:

> The iVotronic contains a VVPAT printer on all machines. In this instance, ES&S has implemented a "continuous roll" VVPAT, meaning that each ballot image is captured in the order in which it is voted on a continuous roll. The use of this type of VVPAT allows a complete violation of voter privacy.
>
> The "numbered list of voters" is a list of voters listed in the order in which they voted. This document is considered public information and is available for inspection by the public at each county board of elections upon request. Furthermore, nothing prevents a volunteer authorized by a candidate or political party as a "watcher" from remaining all day in the polling place and recording the order of voters, and, if necessary, the specific machine on which they voted. Because the ballot images are recorded on paper in the order in which they are voted, merely comparing each ballot image with the numbered list of voters will reveal every voter's choices in a given precinct. Such a comparison could easily be made in the event of a recount. This is a direct violation of Article VII, Section 4 of the Pennsylvania Constitution, which mandates that "[a]ll elections by the citizens shall be by ballot or by such other method as maybe prescribed by law; Provided, That secrecy in voting be preserved." This also violates section 1107-A(1) of the Election Code, 25 P.S . § 3031 .7(1), which states that no electronic voting system can be approved unless it "provides for voting in absolute secrecy and prevents any person from seeing or knowing for whom any voter, except one who has received or is receiving assistance as prescribed by law, has voted or is voting." **Due to these requirements, the iVotronic continuous roll VVPAT must be disabled prior to being delivered to counties because it violates the Pennsylvania Constitution and the Election Code.**

"Examination of the Election Systems and Software, Inc. iVotronic Touchscreen Voting System with Unity Software: A Report by the Secretary of the Commonwealth of Pennsylvania," December 2005.

- Similar concerns appear in a report written by James Sneeringer, a voting system examiner for the State of Texas, considering the certification of the same Hart InterCivic eSlate system that has been certified in Colorado. Sneeringer writes:

> Hart's VVPAT system has one inherent weakness. There is a possible compromise of privacy, because the paper records for each voting station are stored in the order that people vote. For example, if everyone in a precinct votes on a single DRE, comparing the VVPAT tape to the voter

> sign-in log would reveal how people voted. Even with multiple machines, a poll watcher could record the order in which people vote on a given machine. If the VVPAT tape is an open record under Texas law, then the Hart VVPAT appears to violate Texas law.
>
> **Recommendation**. This problem needs to be considered and addressed by the Secretary of State and the Legislature. This type of VVPAT is only acceptable if the VVPAT tape is not an open record, and procedures are in place to protect the privacy of the tape. Possibly the tape would only be opened in the event of a contest, and only under controlled circumstances. Also, standards and procedures should be developed for VVPAT use in Texas.

James Sneeringer, Ph.D., "Voting System Examination: Hart InterCivic," June 2006, available at http://www.sos.state.tx.us/elections/laws/may2006_hart.shtml.

This same concern is echoed by another Texas examiner:

> Because the tape is continuous, voter anonymity could be compromised if the signature roster was used with the tape. I did not take apart the VVPAT module to determine if a seal would need to be broken in order to view the tape.

Tom Watson, "Hart InterCivic," June 2006, available at http://www.sos.state.tx.us/elections/laws/may2006_hart.shtml.

- While Colorado statutes differ from Pennsylvania and Texas, the concerns raised in these other states certainly apply in Colorado. Colorado Election Rules require:

> The Election Official shall put measures in place to protect the anonymity of voters choosing to vote on DREs during the voting periods. These measures shall include:
>
> b) Appropriate marking in Poll Book or other voting list indicating voters choice to vote on DRE with the words: "Voted DRE", or similar in place of paper ballot information. No record shall be kept indicating the order in which people voted on the DRE, or which V-VPAT record is associated with the voter.

8 C.C.R. § 1505-1 (11.6.2.1).

> The V-VPAT system shall be designed in conjunction with State Law to ensure the secrecy of votes so that it is not possible to determine which voter cast which paper record.

8 C.C.R. § 1505-1 (45.5.2.9.11).

When the VVPAT record inherently reflects the order in which the votes were cast, the privacy and secrecy requirements are violated, even if the Election Rules require the local "Election Official" to take measures to prevent poll workers from recording the order in which electors voted. The Election Officials can do little, if anything, to prevent unofficial poll observers from capturing the order in which voters cast their vote, and this general precaution is both insufficient and ridiculous, particularly when purely technological solutions to ensure voter privacy can be implemented with only marginal additional expense.

- Other VVPAT technologies are certainly possible. For example, a VVPAT printer could either include a cutting device, to separate ballots, or it could print on distinct ballot cards, either of which would then fall into a hopper to store the votes. Such cutting devices are a standard feature in commercial receipt printers. The addition of a physical "shaking" step would be sufficient to randomize the ballots. Likewise, machine-printed and hand-carried ballots, delivered to a traditional ballot box (as used in the ES&S AutoMark voting system), would also offer satisfactory ballot randomization. Colorado's election statutes contemplate better VVPAT technologies than the continuous-roll paper systems currently certified for use in Colorado elections, and there's no reason that the subject vendors could not design and offer such systems.

Finally, an important property of any voting system is that it not have any more ballots recorded than there were voters who cast a ballot. If a voting machine were to cast additional ballots, silently while nobody was watching, this would represent a significant security problem. With paperless DRE systems, a significant risk is that either malicious software tampering or simple software bugs could corrupt the electronic storage of the votes. The VVPAT is intended to address this by having a voter physically observe a tangible recording of their vote. Should such a vulnerability exist in the design of the voting systems' software, existing paper-roll VVPAT systems provide no interlocks or other physical mechanisms that would prevent a machine from casting a large number of fraudulent votes. While this would hopefully be detected in post-election auditing, particularly if the number of votes in a precinct outnumbered the number of voters, there would be no way to separate the legitimate votes from the fraudulent votes. This contrasts with systems where unmarked paper ballots are handed to voters by poll workers. Any ballot box stuffing requires the action of humans. Of course, we know people can stuff ballots by hand as well. An electronic VVPAT system that includes a manual, interlocking step is one way of limiting the damage that could result from a corrupt voting machine and would have stronger security than current continuous-roll systems. While Colorado's rules do not explicitly require a manual step or interlock, they do require that it not be possible to "[introduce] data for a vote not cast by a registered voter" (45.5.2.6.1 (g)). As one of the VVPAT's purposes is to mitigate against software tampering or bugs that would otherwise allow this requirement to be violated, the present paper-loop VVPAT systems violate this requirement.

## III. 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 medical and scientific literature, is attached as Exhibit B.

## V. 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,

Dan S. Wallach, Ph.D.