

DISTRICT COURT, DENVER COUNTY,  
STATE OF COLORADO

City and County Building  
1437 Bannock Street  
Denver, Colorado 80204

**Plaintiffs:**

MYRIAH SULLIVAN CONROY, ROCHELLE D.  
COHEN, JULIEANN MURPHY CROSS, TIMOTHY J.  
CHAPPELL, KATHY DEAN, TONY DELCAVO, ANN  
GOLDSTEIN, MICHAEL MELIO, MICHAEL NEIL,  
WENDY NORRIS, DANIEL PINTO, JEFFREY A.  
SHERMAN, and ROBERT SOTO

**Defendants:**

GINNETTE DENNIS, Secretary of State of the State of  
Colorado, in her official capacity only; THE BOARD OF  
COUNTY COMMISSIONERS FOR THE COUNTY OF  
ADAMS; THE BOARD OF COUNTY  
COMMISSIONERS FOR THE COUNTY OF  
ARAPAHOE; THE BOARD OF COUNTY  
COMMISSIONERS FOR THE COUNTY OF  
BOULDER; THE BOARD OF COUNTY  
COMMISSIONERS FOR THE CITY AND COUNTY OF  
BROOMFIELD; THE BOARD OF COUNTY  
COMMISSIONERS FOR THE COUNTY OF  
DOUGLAS; THE BOARD OF COUNTY  
COMMISSIONERS FOR THE COUNTY OF  
JEFFERSON; THE BOARD OF COUNTY  
COMMISSIONERS FOR THE COUNTY OF LA  
PLATA; THE BOARD OF COUNTY  
COMMISSIONERS FOR THE COUNTY OF LARIMER  
and THE BOARD OF COUNTY COMMISSIONERS  
FOR THE COUNTY OF WELD

**Attorneys for Plaintiffs:**

Paul F. Hultin (Atty. Reg. #0142)  
Andrew C.S. Efaw (Atty. Reg. #29053)  
Michael T. Williams (Atty. Reg. #33172)  
Alissa S. Hecht (Atty. Reg. #36126)  
Andrew H. Myers (Atty. Reg. #34288)  
Ramona L. Lampley (Atty. Reg. #37288)  
Wheeler Trigg Kennedy LLP  
1801 California Street, Suite 3600  
Denver, CO 80202  
Telephone: (303) 244-1800  
Facsimile: (303) 244-1879  
E-mail: hultin@wtklaw.com; efaw@wtklaw.com

▲ COURT USE ONLY ▲

Case No. 06CV

Division

Courtroom

Lowell Finley (*pro hac vice* application pending)  
Law Offices of Lowell Finley  
1604 Solano Avenue  
Berkeley, CA 94707  
Telephone: (510) 290-8823  
Facsimile: (510) 526-5424  
E-mail: lfinley@wwc.com

**COMPLAINT FOR DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF**

Plaintiffs allege as follows:

1. Plaintiffs bring this Complaint for Declaratory Judgment and Injunctive Relief to protect their fundamental rights to vote and the purity of Colorado's elections. Plaintiffs seek a declaration that the Colorado Secretary of State ("Secretary") violated the Colorado Constitution and Colorado Statutes by unlawfully certifying for use in Colorado elections certain Direct Recording Electronic ("DRE") computerized voting systems that do not satisfy state law requirements for reliability, security, accuracy, verifiability, and accessibility to all Colorado voters (the "Subject DREs"). The Subject DREs include DREs manufactured by Diebold Election Systems, Inc. ("Diebold"), Sequoia Voting Systems, Inc. ("Sequoia"), Election Systems and Software, Inc. ("ES&S"), and Hart InterCivic, Inc. ("Hart"). The Subject DREs present unacceptable risks of hacking and vote manipulation, election uncertainty, and incorrect election outcomes.
2. Plaintiffs seek a declaration that it is unlawful for county election officials to purchase, lease, or use the Subject DREs that do not comply with the Colorado Constitution, Colorado Statutes, and regulations, as well as an injunction prohibiting use of the Subject DREs in Colorado elections.
3. The Colorado counties associated with the Defendant County Commissioners plan to use Diebold, Sequoia, ES&S, or Hart DREs, or some combination of these DREs, in statewide elections in 2006 and thereafter.
4. Use of the Subject DREs would violate the Colorado Constitution and Colorado Statutes, would constitute an unconstitutional infringement of Plaintiffs' fundamental right to vote, and would result in electoral chaos and irreparable harm to Plaintiffs' fundamental right to vote and to the integrity and purity of Colorado elections.

### **PARTIES, JURISDICTION, AND VENUE**

5. Plaintiff Myriah Sullivan Conroy is a qualified voter who is registered to vote in Boulder County, Colorado, plans to vote in the 2006 elections, and wishes to have her vote properly counted and weighted in any forthcoming election.

6. Plaintiff Rochelle D. Cohen, M.D. is a qualified voter who is registered to vote in Arapahoe County, Colorado, plans to vote in the 2006 elections, and wishes to have her vote properly counted and weighted in any forthcoming election.

7. Plaintiff Julieann Murphy Cross is a qualified voter who is registered to vote in Adams County, Colorado, plans to vote in the 2006 elections, and wishes to have her vote properly counted and weighted in any forthcoming election.

8. Plaintiff Timothy J. Chappell is a qualified voter who is registered to vote in Weld County, Colorado, plans to vote in the 2006 elections, and wishes to have his vote properly counted and weighted in any forthcoming election.

9. Plaintiff Kathy Dean is a qualified voter who is registered to vote in Arapahoe County, Colorado, plans to vote in the 2006 elections, and wishes to have her vote properly counted and weighted in any forthcoming election.

10. Plaintiff Tony Delcavo is a qualified voter who is registered to vote in Douglas County, Colorado, plans to vote in the 2006 elections, and wishes to have his vote properly counted and weighted in any forthcoming election.

11. Plaintiff Ann Goldstein is a qualified voter who is registered to vote in Boulder County, Colorado, plans to vote in the 2006 elections, and wishes to have her vote properly counted and weighted in any forthcoming election. Ms. Goldstein is legally blind and wishes to vote independently and privately in future elections.

12. Plaintiff Michael Melio is a qualified voter who is registered to vote in Jefferson County, Colorado, plans to vote in the 2006 elections, and wishes to have his vote properly counted and weighted in any forthcoming election.

13. Plaintiff Michael Neil is a qualified voter who is registered to vote in the City and County of Denver, Colorado, plans to vote in the 2006 elections, and wishes to have his vote properly counted and weighted in any forthcoming election. Mr. Neil has paraplegia, significant impairment to the mobility and dexterity of his upper extremities, and wishes to vote independently and privately in future elections.

14. Plaintiff Wendy Norris is a qualified voter who is registered to vote in Larimer County, Colorado, plans to vote in the 2006 elections, and wishes to have her vote properly counted and weighted in any forthcoming election.

15. Plaintiff Daniel Pinto is a qualified voter who is registered to vote in the City and County of Denver, Colorado, plans to vote in the 2006 elections, and wishes to have his vote properly counted and weighted in any forthcoming election.

16. Plaintiff Jeffrey A. Sherman is a qualified voter who is registered to vote in the City and County of Broomfield, Colorado, plans to vote in the 2006 elections, and wishes to have his vote properly counted and weighted in any forthcoming election.

17. Plaintiff Robert Soto is a qualified voter who is registered to vote in La Plata County, Colorado, plans to vote in the 2006 elections, and wishes to have his vote properly counted and weighted in any forthcoming election.

18. Defendant Ginnette Davis is the Colorado Secretary of State, a public officer of the State of Colorado and is named as Defendant in this action in her official capacity only. The Secretary is the public officer responsible for the conduct of statewide elections.

19. Defendant Board of Commissioners for County of Adams, Colorado (“Adams County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The Adams County Board is responsible for the conduct of elections in Adams County.

20. Defendant Board of Commissioners for County of Arapahoe, Colorado (“Arapahoe County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The Arapahoe County Board is responsible for the conduct of elections in Arapahoe County.

21. Defendant Board of Commissioners for County of Boulder, Colorado (“Boulder County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The Boulder County Board is responsible for the conduct of elections in Boulder County.

22. Defendant Board of Commissioners for the City and County of Broomfield, Colorado (“Broomfield County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The Broomfield County Board is responsible for the conduct of elections in Broomfield County.

23. Defendant Board of Commissioners for County of Douglas, Colorado (“Douglas County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The Douglas County Board is responsible for the conduct of elections in Douglas County.

24. Defendant Board of Commissioners for County of Jefferson, Colorado (“Jefferson County Board”), is a public board of this State and is named as Defendant in this action in its

official capacity. The Jefferson County Board is responsible for the conduct of elections in Jefferson County.

25. Defendant Board of Commissioners for County of La Plata, Colorado (“La Plata County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The La Plata County Board is responsible for the conduct of elections in La Plata County.

26. Defendant Board of Commissioners for County of Larimer, Colorado (“Larimer County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The Larimer County Board is responsible for the conduct of elections in Larimer County.

27. Defendant Board of Commissioners for County of Weld, Colorado (“Weld County Board”), is a public board of this State and is named as Defendant in this action in its official capacity. The Weld County Board is responsible for the conduct of elections in Weld County.

28. This Court has jurisdiction over this action pursuant to the Colorado Constitution and C.R.S. § 13-1-124.

29. Under Colorado Rule of Civil Procedure (“C.R.C.P.”) 98, venue is appropriate in the City and County of Denver, Colorado.

30. Plaintiffs bring this action pursuant to C.R.S. § 13-51-101 *et seq.*, the Uniform Declaratory Judgments Act, and Rules 57, 65, and 106 of the Colorado Rules of Civil Procedure. An actual controversy exists between Plaintiffs and Defendants regarding Defendants’ non-compliance with the Colorado Constitution, C.R.S. § 1-5-601.5 *et seq.*, and related statutes and regulations.

### **GENERAL ALLEGATIONS**

31. According to the United States Government Accountability Office (“GAO”), most American voters now vote using one of two types of electronic voting systems, either optical scan systems or Direct Recording Electronic (“DRE”) systems. These systems typically include the hardware, software, and firmware used to define ballots, cast and count votes, report and display election results, and maintain and produce audit trail information, if any.

32. Optical scan voting systems tabulate paper ballots, often using the same “mark-sense” technology that is used for scoring standardized tests. The official ballot in optical scan systems usually is the paper ballot itself, not the electronic record generated by the electronic tabulating machine.

33. DREs, on the other hand, capture votes electronically, without the use of paper ballots. DREs come in two basic models: pushbutton or touch-screen.

34. Like any computer, a DRE and its components, such as memory cards, are vulnerable to security breaches, or hacking, from the vendor's insiders or from outsiders. A hacker who breaches or compromises a DRE machine's security can alter the results of an election in a manner that is not detectable to election officials.

35. When a computer programmer creates a computer program, he or she writes it in human-readable code. This is known as the "source code." That source code is then run through a program called a "compiler," which translates the source code into machine-readable code called "object code." There is often an additional step required that is called "linking" or "binding." For that step, the object code is run through a linking or binding program, and the result is the executable program—the machine-readable instructions to the computer. When a computer program is installed on a machine, the codes are loaded onto the machine and stay there. After the program is installed, if the source code, object code, compiler, and linking program are deleted from the machine, only the machine-readable code remains on the computer, making it difficult for humans to alter the executable program.

36. Interpreted code is written in a human-readable format similar to source code. Interpreted code remains in human-readable format on the machine where it is run. A computer program called an "interpreter," which remains on the machine at all times, reads the interpreted code and translates the code into machine-readable format each time the program runs. Thus, with interpreted code, human-readable code and an interpreter are present on the machine, and it is easy for a knowledgeable person to alter that interpreted code. In the case of a computer program in a DRE voting system, alteration of the interpreted code can result in election fraud and alteration of election results.

37. To support and provide some measure of voter verification for DREs, several different kinds of voter verified paper recording devices ("VVPR") have been developed and are in various stages of deployment. The two predominant VVPRs are reel-to-reel voter verified paper audit trails ("VVPATs") or voter verified paper ballots ("VVPBs"). Colorado uses a VVPAT system pursuant to Colorado Election Rule ("C.E.R.") 45.5.2.20 and C.R.S. § 1-1-104(50.6)(a).

38. Congress passed the Help America Vote Act of 2002 ("HAVA"), which contains a number of provisions designed to reform the way Americans vote. Pursuant to HAVA, Congress has appropriated funds to be used by the States for the improvement of voting systems, but that funding is conditioned on the States' replacement of all punch card and lever machines, which had to be replaced by January 1, 2006.

39. HAVA also created the United States Election Assistance Commission ("EAC"), whose duties include promulgating voluntary guidelines for voting machines. Section 222(e) of HAVA provides that the 2002 Voluntary Voting System Standards ("VVSS") adopted by the

Federal Election Commission (“FEC”) are deemed to be adopted by the EAC as the first set of voluntary voting system guidelines adopted under HAVA. The VVSS set out standards that provide guidance to voting machine manufacturers, independent testing authorities, and the states regarding various features of voting systems. Among the features addressed in the VVSS are security features. One of the VVSS provisions designed to minimize security problems is the prohibition of “interpreted code” in electronic voting systems, including DREs.

40. The VVSS prohibit the presence of human-readable computer code in DRE voting systems, including interpreted code. This prohibition reduces a DRE voting system’s vulnerability to hacking.

41. Pursuant to Section 301(a)(3) of HAVA, each polling place in a federal election must have at least one voting system that allows voters with disabilities, including blind and visually impaired voters, to vote privately and independently. These machines must be in place for the 2006 elections.

42. Colorado is spending its federally appropriated HAVA funds and attempting to meet HAVA requirements with the purchase of DREs and related equipment and software.

43. Article VII, Section 11 of the Colorado Constitution provides: “The general assembly shall pass laws to secure the purity of elections, and guard against abuses of the elective franchise.” The Colorado General Assembly has passed legislation designed to secure the purity of this State’s elections and to guard against abuses of the elective franchise. The Colorado Secretary of State, among other public officials, must comply with and implement such laws.

44. In furtherance of the General Assembly’s obligations under the Colorado Constitution, the State has adopted legislation that incorporates and adopts all HAVA standards, regulations, and requirements as a matter of Colorado law.

45. Colorado’s statutory requirements for electronic voting systems are found in Article 5, Part 6 of the Elections Code, titled “Authorization and Use of Voting Machines and Electronic Voting Systems.” C.R.S. § 1-5-601.5 *et seq.* Pursuant to C.R.S. § 1-5-601.5, all electronic voting systems and voting equipment offered for sale in this State on or after May 28, 2004, must meet the 2002 VVSS promulgated by FEC and adopted by EAC, as well as any voluntary standards promulgated thereafter by EAC.

46. Colorado Revised Statute § 1-5-616 requires the Secretary to adopt minimum standards for a number of technical specifications for certification of electronic voting machines. These minimum standards, to the extent they have been considered by the Secretary, are set forth in the Colorado Election Rules (“C.E.R.”), 8 C.C.R. § 1505-1. Among other things, the Secretary must establish minimum standards for “evaluation criteria” and “security requirements” for electronic voting systems. C.R.S. §§ 1-5-616(1)(e), 616(1)(g).

47. The Secretary has failed to comply with Colorado Statutes and regulations governing elections and election equipment. For example, in contravention of her statutory duty to establish minimum security requirements for electronic voting systems, the Secretary has delegated to private vendors all authority to establish and document minimum security requirements for such systems. *See* 8 C.C.R. § 1505-1 (45.5.2.6.1) (“The voting system provider shall provide documentation detailing voting system security in the areas listed below. . . .”); 8 C.C.R. § 1505-1 (45.5.2.6.2) (“The voting system provider shall submit to the [Secretary] its recommended policies or guidelines governing . . . .”); 8 C.C.R. § 1505-1 (45.5.2.6.3) (“The voting system shall include detailed documentation as to the security measures it has in place for all systems, applicable software, devices that act as connectors (upload, download, and other programming devices), and any security measures the voting system provider recommends to the end users that purchase the voting system.”).

48. The Secretary has failed to establish any minimum standards for evaluation criteria. The State standards in Colorado Election Rule 45 pertaining to Voting Systems Standards for Certification are completely silent as to the evaluation criteria to be used in determining whether a DRE is secure or reliable.

49. The Colorado Statutes and Election Rules require the Secretary to produce a certification report, a qualification report, and a certification document for each electronic voting system after completion of the Secretary’s functional testing of such systems. The certification report is to be completed within 30 days after the Secretary decides to certify an electronic voting system. C.R.S. § 1-5-617(4). The qualification report and certification document are to be prepared within 21 days after completion of the Secretary’s functional testing of the electronic voting system. 8 C.C.R. § 1505-1 (45.3.3(d)).

50. Pursuant to an Open Records Act request, the Secretary has produced to Plaintiffs its public records relating to the testing and certification of the Subject DREs. The records were produced in a chaotic and incomprehensible manner. Based on the manner in which the records were produced, it is impossible to determine what tests, if any, were conducted by the Secretary in certifying each of the Subject DREs. It also is impossible to determine the identities of the experts, if any, that the Secretary appointed “to assist [the Secretary] in the examination and testing of electronic or electromechanical voting systems submitted for certification and to produce a written report on each system.” C.R.S. § 1-5-617(2).

51. Upon information and belief, the Secretary has not yet prepared a certification report or a qualification report for the Subject DREs that have been certified by the Secretary and that are being purchased for use by various Colorado counties in the 2006 elections. The Secretary’s apparent failure to comply with Colorado Statutes and her own Election Rules evidences the Secretary’s failure to certify electronic voting systems that comply with state and federal laws.

## **DREs Are Inherently Untrustworthy**

52. A basic tenet of computer science is that program testing can be used to show the presence of bugs or malicious code, but never to show or prove the absence of bugs or malicious code. In fact, it is impossible to prove that any computer is not infected with malicious code. This tenet holds true for DREs. No matter how stringent the testing and certification may be, no electronic voting system will be 100% secure or 100% reliable. This fundamental fact makes it necessary to utilize permanent paper ballots in connection with any electronic voting system so that the paper ballots can be used to audit the electronic systems and to recount the ballots, if necessary. And this fundamental fact is especially important in the present circumstances, where the Subject DREs are far, far from 100% secure or 100% reliable.

53. Because DREs operate invisibly in electronic circuits, it is possible for a voter to vote for candidate "A," for the DRE to display a vote for candidate "A," but record a vote for candidate "B." Only the voter knows he or she voted for "A," and he or she will never know of the miscount unless no votes at all are reported for candidate "A."

54. Voters have no means to confirm that DREs have recorded their votes correctly, nor can they have any assurance of that their votes will not be electronically changed or deleted after they have cast their electronic ballots.

55. DREs have experienced problems with unintended "undervotes"—*i.e.*, a voted electronic ballot on which no vote was recorded for a particular race, even though the voter intended to, and believed he or she did, vote for a candidate in that race. Unintended undervotes on electronic ballots can affect the integrity and outcome of an election.

56. An unusually high rate of such undervotes has been recorded on DREs in recent elections as compared to the rate of undervotes recorded by non-DRE systems, such as optical scan systems.

57. DREs and the associated tabulation software may also record "phantom votes," which occur when there are more votes counted for a particular race or ballot issue than the number of voters who actually voted. Phantom votes are problematic as they both dilute the votes of actual voters and mask the problem of undervotes. Phantom votes can affect the integrity and outcome of an election.

58. DREs also can produce "switched votes." A switched vote occurs when the voter attempts to vote for Candidate "X," but the screen or the unseen electronic ballot indicates that the voter selected Candidate "Y" instead. Vote switching impairs a voter's ability to cast a vote for a candidate of his or her choice and produces inaccurate results. Switched votes can affect the integrity and outcome of an election.

59. The GAO has documented security experts' concerns that DRE "testing cannot determine . . . how the system would react in the face of an active attack. Specifically, security

experts argue that functional testing is unlikely to ever trigger certain types of hidden code. As a result, malicious code could be present in a system and evade testing as long as the triggering commands were not entered.” GAO, *Elections: Federal Efforts to Improve Security and Reliability of Electronic Voting Systems Are Under Way, but Key Activities Need to Be Completed* (Sept. 2005).

60. According to the GAO, multiple recent reports, including several state-commissioned technical reviews and security assessments, have voiced concerns about the development of secure and reliable DREs. Substantial evidence exists showing that some of these concerns have been realized and have caused problems with recent elections, resulting in the loss and miscount of votes.

61. The GAO has documented findings by state election reviewers showing that values used to encrypt DRE election data were actually defined in the machine’s source code, allowing a hacker to access encrypted data. Several reviewers reported that “smart cards,” which are used to activate the display screen on DRE systems, were not secured by some electronic voting systems. Reviewers were able to exploit this weakness by altering such cards and using them to improperly access election “administrator” functions, vote multiple times, change vote totals, and produce false election reports in a test environment.

62. The GAO has further noted that several evaluations have demonstrated that election management systems did not encrypt the data files containing electronic “cast vote” records, leaving the electronic votes subject to viewing or modification.

63. Evaluations have shown that current DRE software is subject to access by other computer programs, permitting untraceable alteration of the cast vote records. Computer experts have demonstrated that, with minimal effort, they can hack into the ballot definition files and alter them so that the votes shown on the display screen for one candidate would actually be recorded and counted for a different candidate. Further, these experts have demonstrated the electronic voting systems’ vulnerability to attacks by *outsiders* and have not even begun to address the systems’ more critical vulnerability to attacks by *insiders*—namely, the private vendors’ hardware and software engineers, programmers, and other employees or agents who are granted access to the systems’ hardware, firmware, and software during the design, manufacture, deployment, and field support of the electronic voting systems.

### **The DREs to Be Used in Colorado’s 2006 Elections Are Inherently Untrustworthy**

64. The Secretary has certified DREs manufactured by Diebold, Sequoia, ES&S, and Hart for statewide elections in 2006 and thereafter.

65. Each voting system certified in Colorado must meet the qualifications of EAC’s 2002 VVSS, be certified by an independent testing authority (“ITA”) that is certified by the National Association of Election Directors, and pass the State of Colorado Voting Systems Certification Program. C.E.R. 37.4.

66. The Secretary has certified a Diebold DRE both for use in the 2006 elections and thereafter. Specifically, the Secretary authorized the Diebold AccuVote-TSX DREs and associated components.

67. County election officials in Adams, Broomfield, La Plata, Larimer, and Weld Counties plan to or already have purchased the above Diebold DRE system.

68. The Secretary has certified a Sequoia DRE both for use in the 2006 elections and thereafter. Specifically, the Secretary authorized the Sequoia AVC Edge DRE and associated components.

69. County election officials in Arapahoe County plan to or already have purchased the above Sequoia DRE system.

70. The Secretary has certified an ES&S DRE both for use in the 2006 elections and thereafter. Specifically, the Secretary authorized the ES&S iVotronic DRE and associated components.

71. County election officials in Jefferson County plan to or already have purchased the above ES&S DRE system.

72. The Secretary has certified a Hart DRE both for use in the 2006 elections and thereafter. Specifically, the Secretary authorized the Hart eSlate DRE and associated components.

73. County election officials in Boulder and Douglas Counties plan to or already have purchased the above Hart DRE system.

74. The Subject DREs purchased or leased by Colorado counties may malfunction and lose, add, or misdirect votes.

#### **Diebold DREs**

75. Diebold DREs, which are to be used in Adams, Broomfield, La Plata, Larimer, and Weld Counties, have a history of well-known security flaws and are currently being challenged in several States, due to the Diebold DREs' lack of security, including the presence of illegal interpreted code and the potential for faulty reporting of votes.

76. The Diebold touch-screen DRE voting systems that Adams, Broomfield, La Plata, Larimer, and Weld Counties plan to purchase (or already have purchased) and use have serious flaws that leave them vulnerable to election fraud through software tampering.

77. In 2003, Dr. Aviel Rubin of Johns Hopkins University and his research team analyzed the publicly available source code for the Diebold AccuVote-TS DRE, which is the predecessor DRE to the Diebold AccuVote-TSX certified for use in Colorado. Dr. Rubin's team

found significant security flaws in that voters could cast multiple ballots and regular voters could perform administrative functions.

78. In September 2003, Science Application International Corporation (“SAIC”) issued a “Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes,” which was commissioned by the Governor of Maryland. The report identified 328 security flaws and concluded that “the system, as implemented in policy, procedure, and technology, is at high risk of compromise.”

79. In December 2003, the Ohio Secretary of State released its “DRE Technical Security Assessment” and found that the Diebold AccuVote-TS voting system had more security risks rated “high” than any other vendor’s system. The report stated that the same PIN—1111—was used on all “supervisor” smart cards nationwide, and that an unauthorized person could use the PIN to gain access to supervisor functions on the voting terminal.

80. In January 2004, the Maryland Department of Legislative Services released a report titled “Trusted Agent Report: Diebold AccuVote-TS Voting System,” which was prepared by RABA Technologies, LLC. The RABA report identified numerous security vulnerabilities in the Diebold GEMS tabulation software and concluded that “a pervasive rewrite” of Diebold’s code would be required to significantly improve its security.

81. The California Secretary of State concluded in a special report on California’s March 2004 elections that Diebold DREs experienced operating problems that severely curtailed voting in San Diego County and significantly affected voting in Alameda County, and that Diebold never alerted California election officials about this equipment problem, nor provided poll worker training to address the problem. Due to the Diebold DRE failures, voters were sent away or to other polling places. As a result, the California Attorney General investigated Diebold for criminal fraud charges and obtained a \$2.6 million False Claims Act settlement.

82. The Diebold AccuVote-TSX DRE and the Diebold AccuVote-OS optical scan system, certified by the Secretary for use in the 2006 elections and thereafter, use substantially the same removable memory cards as key parts of their systems. Those memory cards contain:

- a. The election description (*i.e.*, races, candidates, parties, propositions, and ballot layout);
- b. Vote counters for every candidate and proposition;
- c. Byte-coded object programs;
- d. The internal electronic audit log;
- e. An election mode field indicating whether the system containing the card is currently being used in a real election; and

f. Other variables and data describing the state of the election.

83. In 2005, computer security investigator Harri Hursti was permitted to investigate Diebold's AccuVote-OS voting machine. Dr. Hursti demonstrated that a person with access to a Diebold AccuVote-OS system's removable memory card—the same card used in the Diebold AccuVote-TSX DREs—could modify scripts (small programs written in Diebold's proprietary AccuBasic source code) that are stored on the card, and also could alter the vote counts stored on the card in a manner that would affect the outcome of the election and not be detected by the post-election canvass procedures.

84. Concern over Dr. Hursti's report prompted the California Secretary of State to order its Voting Systems Technology Assessment Advisory Board ("VSTAAB") to conduct an analysis of the AccuBasic source code for both the AccuVote-OS and the AccuVote-TSX DRE. David Jefferson of Lawrence Livermore Laboratories and University of California Computer Science Professors David Wagner and Matt Bishop authored the official VSTAAB report. Their report highlighted the following concerns:

a. Anyone who has access to the memory card of the AccuVote-OS and can modify its contents can modify the election results in a number of ways without allowing detection except through a recount of actual paper ballots;

b. Sixteen bugs in the implementation of Diebold's AccuBasic interpreter could allow an attacker to change vote totals, modify reports, change the names of candidates, change the races voted on, or insert his own code into the running firmware of the machine;

c. The only way to detect such attacks on the AccuVote-OS is through recounting the original paper ballots;

d. The bugs in the AccuVote-OS are also present in the Diebold AccuVote-TSX DRE;

e. Implementation of cryptographic protection in the AccuVote-TSX is flawed. The AccuVote-TSX uses a default key, which is hard-coded into the source code for every such machine in the United States and has been openly published for over two years on the Internet;

f. The AccuBasic interpreter does not appear to have been written using high-assurance development methodologies;

g. Interpreted code is prohibited by the 2002 VVSS, currently adopted by the EAC as its first set of voting system standards, and by the EAC's updated Voluntary Voting System Guidelines due to take effect in 2007.

85. The Diebold DREs' interpreted code is a particularly serious security risk because it is loaded at the time of the election in "real time," not in advance, and is not subjected to security testing and certification. The Diebold DREs' interpreter is accessible on the Diebold memory card, which is small and portable. Anyone with access to the interpreted code can change it before, during, or after an election.

86. The danger that these memory cards could be tampered with while they are in the AccuVote-TSX units is particularly high because the AccuVote-TSX's Windows CE operating system has never been subjected to testing by any ITA.

87. In 2006, Dr. Hursti was allowed to examine the Diebold AccuVote-TSX DRE, and the security vulnerability he discovered has rocked the computer security world. Dr. Hursti found that he could readily install malicious code permanently on the machine at the most fundamental level that can defeat any attempt to secure the machine afterwards.

88. There are three levels of code in any computer: the BIOS (that interfaces the hardware to the software, controls the system at startup, and is the basic level of machine functionality), the operating system (that provides essential services, including security, for the system), and the application (in this case, voting functionality).

89. The BIOS is what a computer user is working with when a computer starts up and offers the user the option to press F2 or some other key and set things like the boot sequence, the system clock, the processor speed, and some hardware level functions, including some security functions.

90. In a report now referred to as "Hursti II," Dr. Hursti showed that he could easily alter the Diebold BIOS (the most fundamental level in any computer) and attack both the operating system and voting application of the Diebold AccuVote-TSX as well. All it takes is a standard PC memory card, naming the files according to Diebold's naming scheme, and gaining brief physical access (a minute or two) to the AccuVote-TSX machine. The system will automatically install the malicious code, which can be permanent, can contain functionality to enable further attacks (such as vote reallocation), can protect itself from forensic investigation, and can defeat any security measures added at a higher level (such as hash code checking).

### **Sequoia DREs**

91. Sequoia touch-screen DREs come in several different versions: the original AVC-Edge (sometimes referred to as the Edge I), the Edge II, the Edge I or II with Veri-Vote Printer, and the Edge II Plus.

92. The Sequoia DRE voting systems that Arapahoe County plans to purchase and use have serious flaws that leave them vulnerable to election fraud through software tampering.

93. In 2003, a study by Compuware Corporation for the Ohio Secretary of State identified several significant security issues. The most significant risks included the following:

a. The Sequoia AVC-Edge DREs can be placed in supervisor mode, which allows the user to take control of the machine, using a button on the back of the DRE. Supervisor functions are not password protected, and therefore, an unauthorized person can enter supervisor mode;

b. No password is required to close the polls; therefore, there is a risk that an unauthorized person might close the polls, preventing others from voting;

c. The power switch on Sequoia AVC-Edge DREs is not protected by a lock or seal. It is accessible on the back of the unit. An unauthorized person can power off the DRE during voting; and

d. Sequoia AVC-Edge DREs use standard memory cards for storing the ballot definitions and vote results. These cards can be placed in a laptop and altered.

94. All versions of the Sequoia Edge DREs are used in conjunction with Sequoia's WinEDS election management software. WinEDS runs on a server computer and is used to create election and ballot information for each election to download into the DREs and also to tally and produce reports of election results uploaded from the Edge units following an election.

95. Jeremiah Akin, an expert computer programmer, has demonstrated the serious security vulnerabilities in the Sequoia WinEDS election management software after discovering a full working copy of the executable code for WinEDS on an unprotected Internet site.

96. On a laptop computer, Mr. Akin was able to modify the software in several different ways, each of which would change election results and then automatically remove any detectable trace of the changes.

97. Other experts have independently verified Mr. Akin's work and opined that the security vulnerabilities in the Sequoia WinEDS program are real and do in fact allow undetectable alteration of election results in as few as ten minutes.

### **ES&S DREs**

98. The ES&S iVotronic DRE that Jefferson County plans to purchase and use has serious flaws that leave it vulnerable to election fraud through software tampering.

99. The ES&S iVotronic DRE is a touch-screen voting system that, along with accompanying election management software, is called the "Unity system."

100. A recent study conducted by the Pennsylvania Secretary of the Commonwealth identified potential security problems in the ES&S iVotronic DRE. They include the following:

- a. ES&S iVotronic DRE modules can be set so that they do not require passwords;
- b. Factory-set default passwords can be used on any ES&S iVotronic DRE in the country;
- c. ES&S iVotronic DRE memory cards, containing audio and long text ballots, can be installed at the polling place, compromising the security of the memory card and permitting the possibility that counterfeit cards could be substituted;
- d. There are accessible, unsecured cable connections at the top edge of ES&S iVotronic DREs; and
- e. The ES&S Unity tabulating software runs on a Windows platform that, if used with a modem, could allow untraceable connections to the Internet, connection of the ES&S system with uncertified telephone equipment, and the introduction of malicious code into the ES&S system.

101. Any person with knowledge of a poll worker's trivial ES&S password could irrevocably erase all votes in an ES&S DRE, at any time during a polling day.

102. The Ohio Secretary of State also performed an analysis of the security of the ES&S iVotronic DRE and identified the following as-yet-unmitigated risk: The "add to" feature in the tally program, which is intended to recover data from broken machines, can be executed multiple times for the same machine, and thereby allow overcounting of votes.

### **Hart DREs**

103. The Hart eSlate DRE that Boulder and Douglas Counties plan to purchase and use have serious flaws that leaves it vulnerable to election fraud through software tampering.

104. The Hart eSlate DREs, though less widely used and documented than the other vendors' DREs, suffer deficiencies similar in scope and severity to those in the DREs discussed above and inherent to all DREs.

105. In 2005, the Ohio Secretary of State retained Compuware Corporation to perform a security assessment of the security and vulnerability of the Hart eSlate DRE. In its September 16, 2005, report, Compuware identified the following potential vulnerabilities or risks:

- a. The Ballot Origination Software System™ ("BOSS"), which is the Hart software application that enables election officials to build election databases, format ballots, and electronically write ballot formats to Hart's Mobile Ballot Boxes™ ("MBBs") (the PC memory card that carries the election database and formatted ballots to various components of the eSlate DRE system, and the Tally™ software, which is the application that tabulates and reports accumulated vote totals using the Cast Vote Records

("CVRs") recorded on the MBBs, do not utilize encrypted passwords, but instead store user passwords as plain text. Also, the database access IDs and passwords are compiled into the PowerBuilder application and are viewable using the TextPad editor;

b. Locks were not in place to secure the MBB memory card on the Judge's Booth Controller ("JBC"), the polling place control console that election workers use to manage up to 12 eSlate voting terminals, print access codes and voter receipts for individual voters, and records CVRs (*i.e.*, electronic ballot records);

c. The password for the eSlate terminals is a default from Hart;

d. Hart does not use encryption to protect its audit log data on the eSlate and JBC units;

e. While the MBB memory cards are in transit from a polling place to a central election location, the MBBs' programs or files could be corrupted (*e.g.*, so that the electronic ballot records could not be read at the central election facility); and

f. Each JBC control console can have up to 12 eSlate voting terminals attached. Because the eSlate terminals are daisy chained to the JBC, interference with or malfunction of one machine in the eSlate chain could prevent the other eSlate machines from transferring CVRs to the JBC. For example, if the first machine in a sequence of 12 eSlates is unplugged, the votes for the remaining 11 eSlate machines will not transfer to the JBC.

106. Problems with Hart eSlate systems have been reported by other States that have used eSlates. For example, in the State of Texas's March 2006 primary elections, some counties experienced problems with Hart eSlate DREs. In Tarrant County, Texas, a programming error counted some votes multiple times and boosted the final vote tally in two primaries by as much as 100,000 votes.

### **The Subject DREs Provide Inadequate Auditing**

107. Colorado Revised Statute § 1-5-615 requires that the voting system produce a corresponding paper record with audit capacity, and that the paper record must be available for any recount conducted for any election in which the system is used. *See also* 8 C.C.R. § 1505-1 (45.5.2.9.8).

108. Colorado Election Rule § 45.5.2.20 requires each newly purchased electronic voting system to produce a VVPR in the form of a VVPAT. The VVPAT must be an auditable paper record that (a) is available for the elector to inspect and verify before the vote is cast; (b) is produced contemporaneously with or employed by any voting system; (c) lists the designation of each office, ballot issue, or ballot question, and the voter's choices in such offices, issues, or questions (if the elector makes no selection in connection with any race, issue, or question, that

fact shall also be noted on the record produced); (d) is suitable for a manual audit or recount; and (e) is capable of being maintained as an election record in accordance with the requirements of C.R.S. § 1-7-802. C.R.S. § 1-1-104 (50.6)(a).

109. The VVPAT must contain a printer that is attached to, built into, or used in conjunction with the DRE. This printer is required to “duplicate a voter’s selections from the DRE onto a paper record.” 8 C.C.R. § 1505-1 (45.5.2.9.3(a)).

110. The VVPAT unit must allow a voter to view his paper record and must store spoiled paper record copies securely. 8 C.C.R. § 1505-1 (45.5.2.9.3). The VVPAT record is the “official record of the election available for recounts” and must “be sturdy, clean, and of sufficient durability to be used for this purpose.” 8 C.C.R. § 1505-1 (45.5.2.9.9).

111. In addition, the VVPAT must be designed to ensure the secrecy of votes so that it is not possible to determine which voter cast the paper record. 8 C.C.R. § 1505-1 (45.5.2.9.11).

112. The VVPAT must allow the voter to verify his vote in the same language in which he voted on the DRE. 8 C.C.R. § 1505-1 (45.5.2.9.13).

113. Upon information and belief, all certified Colorado DREs use reel-to-reel VVPATs.

114. The paper on which these reel-to-reel VVPATs are printed is thermal, continuous roll paper that is similar to cash register receipt paper.

115. VVPATs certified for use in Colorado have not been shown capable of supporting a manual audit as required by Colorado Election Rule 45.5.2.20. The VVPATs are not printed on ballot-quality paper and will not retain their quality during the often-lengthy recount and legal challenge period. The paper is fragile and easily alterable by handling, blackening when it is exposed to heat or sunlight, thereby making it difficult, if not impossible, to read and use for manual audits and recounts.

116. When VVPAT audit trails are recountable, it takes an unacceptably long time to conduct the recount.

a. In Nevada’s 2004 election, 1,268 of 60,000 ballots were audited using a DRE VVPAT reel-to-reel audit trail. The process required five teams of four people two days to complete.

b. In one California VVPAT recount, it took 127.5 hours to recount the 114 ballots—more than one hour for each ballot that was recounted.

c. In July 2005, the California Secretary of State’s office oversaw a “volume test” of the Diebold AccuVote-TSX’s attached printers. The test revealed critical flaws in

the hardware and software of the AccuVote-TSX, including destroyed or lost paper audit records and ongoing software corruptions, which made it possible that votes could be lost or corrupted. In its October 11, 2005, report, the VSTAAB concluded that “any system with failure rates this high is not ready for use in any election.” A second test was held a few months later. This test, which was staffed by California Secretary of State temporary workers and was closely supervised by Diebold staff, concluded that the problems with the earlier test had allegedly been resolved.

117. Additionally, reel-to-reel VVPATs allow for the invasion of voter privacy by preserving the order in which voters have voted.

118. Even when a voter’s choice shows up correctly on the VVPAT, it is impossible for the voter to know whether the official vote has been recorded correctly on the DRE’s memory card, which is the official repository of votes, unless there is a full manual audit that compares the VVPAT to the machine tabulation.

119. For a voter to be unable to properly verify that his or her vote was correctly counted and recorded violates the voter’s fundamental right to vote.

#### **The Subject DREs Provide Inadequate Disability Access**

120. Colorado Election Rule 34.5 provides that when any Colorado “political subdivision acquires a new voting system, the system must be accessible to persons with physical, cultural/educational, mental/cognitive disabilities and provide the voter in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.” 8 C.C.R. § 1505-1 (34.5).

121. Colorado Election Rule 35 provides requirements for voting system accessibility with respect to specific disabilities and mandates that voting systems be accessible to voters with low or no vision, low or no hearing, and limited reach, strength, dexterity, and mobility. It also requires the voting system to provide a tactile-input or speech-input device, and a method by which voters can confirm tactile or audio input by having phonetically accurate audio output back to them. 8 C.C.R. § 1505-1 (35.1.1 - 35.1.2).

122. Likewise, the controls on voting systems must be operable with one hand, including a closed fist, and without tight grasping, pinching, or twisting of the wrist, and the rules provide for maximum reach, height, and stretch positions of the voting device to allow for accessibility for persons in wheelchairs. 8 C.C.R. § 1505-1 (35.1.13 - 35.1.17).

123. The paper record must also be accessible to individuals with disabilities, including nonvisual accessibility, to provide the same opportunity for participation as for other voters, and the voting system must provide alternative language accessibility. 8 C.C.R. § 1505-1 (37.1.5 - 37.1.6).

124. Currently available adaptive technologies for persons with various keyboard impairments and complete inability to use hand controls, which are readily adaptable to voting machines, include, but are not limited to, the following: head switches, foot switches, large “jelly” switches, light-pressure switches, “sip-and-puff” switches, and eye-blink systems.

125. Examples of accommodations for vision-impaired voters include, but are not limited to, the following: audio recordings, magnification of the display screen, the ability to change contrast and color on a display screen, and keypads with Braille numbers or letters on the keys.

126. Mobility and dexterity-related impairments include a wide range of impairments. These impairments range from voters who cannot walk but can use their hands, to voters who lack fine motor control but still have limited use of their hands, to voters who have no use of their hands and legs and must use sip-and-puff breath-controlled devices to cast their votes.

127. Sip-and-puff devices are devices that attach to the voting machine and allow the voter to indicate his or her choices by sipping air from or puffing air into a tube. A sip-and-puff device requires no use of the hands or legs.

128. Jelly switches accommodate voting for dexterity-impaired voters. Jelly switches are large buttons that are easier for a person with limited hand strength and dexterity to press.

129. Cognitive impairments are impairments that make it more difficult for a voter to process information. For example, voters who have suffered strokes will often suffer some degree of cognitive impairment.

130. Voters with cognitive impairments often will require accommodations that allow them to receive information about the ballot in more than one form simultaneously—for example, visually and through spoken messages.

131. Some voters have more than one of the above-described impairments.

132. Upon information and belief, none of the EVS manufactured by Diebold, Sequoia, ES&S, and Hart and certified by the Colorado Secretary complies with Colorado statutory requirements for accessibility for disabled voters.

133. The deficiencies of the Subject DREs certified by the Colorado Secretary include, but are not limited to, the following:

- a. The Subject DREs (other than Hart eSlate DREs, which provides disabled access through its multi-featured, add-on Disabled Access Unit™) do not support standard 2-switch systems or other user interface devices required for use of sip-and-puff, jelly switches, and other assistive devices;

b. Many voters with motor impairments cannot hold the tethered keypads, which are used by the Subject DREs other than the Hart eSlate, in one hand while attempting to press keys with the other. The large size and form factor of these keypads do not facilitate their use as a keypad, held in a single hand and operated by the thumbs of the same hand;

c. The Braille labels beside, above, or below the keys of the keypads are difficult to read. They do not have the Braille dots spaced properly, with the standard Braille dot spacing;

d. The volume controls are of poor quality, noisy, and scratchy. To support the needs of audio voters who have major hearing loss, a high-volume boost capability should be, but is not, available.

e. The Subject DREs (other than the Hart eSlate) do not have a “Call for Help” key or other control to discretely summon assistance from a poll worker.

f. The Subject DREs (other than the Hart eSlate) do not have a 1/8 inch phone jack (separate from the headphone jack) on the keypad, for attaching a sip-and-puff or other standard switched input control device.

g. Many blind, low-vision, and cognitively impaired voters would not be able to navigate successfully through the hierarchical menu system used by most of the Subject DREs.

h. The Subject DREs fail to address the needs of elderly voters who have developed severe visual impairments with age, but who are unfamiliar with, and unable to operate, audio-only access technology because they have had normal vision most of their lives.

i. The audio access functions of the systems also are not suitable for providing accessible voting to voters who are both profoundly hearing impaired and visually impaired. The lack of a standard output interface port means that, for example, a deaf-blind voter cannot bring his or her own portable Braille display device to the polls and plug it into a standard output plug of the Subject DREs, in order to read the instruction materials, mark, review, and correct the ballot privately and independently.

j. Blind and low-vision voters are unable to independently and privately verify their votes using the VVPAT paper trail because the Subject DREs are not equipped with any accommodations allowing blind and low-vision voters to know what is on the VVPAT (without relying on a third party to read it to them).

k. Although technology exists that would allow the Subject DREs certified by the Secretary to comply with Colorado statutory requirements for accessibility for

disabled voters, on information and belief, the Subject DREs purchased by Colorado counties do not include such technology.

### **IRREPARABLE HARM**

134. For all of the reasons set forth in the foregoing paragraphs, if Colorado's counties are permitted to use the Subject DREs in the upcoming Colorado elections, the likely result is electoral chaos: votes are likely to be lost or miscounted (or both), no audit or recount would be possible, and many disabled voters would be denied their statutory rights to vote independently and privately.

135. If Colorado's counties are allowed to use the Subject DREs in the upcoming Colorado elections, that would result in irreparable harm to Plaintiffs' fundamental right to vote and to Colorado's electoral process that is protected by the Colorado Constitution and Statutes.

### **CLAIMS FOR RELIEF**

#### **First Claim for Relief (Declaratory Judgment—Violations of C.R.S. § 1-5-615, 616)**

136. Plaintiffs incorporate the allegations set forth in the foregoing paragraphs of this Complaint as if fully set forth herein.

137. Colorado Revised Statute § 1-5-615 requires that each voting system "counts votes correctly."

138. The Subject DREs certified by the Secretary do not accurately record and count votes.

139. Colorado Revised Statute § 1-5-616 requires the Secretary to adopt rules establishing minimum standards for "evaluation criteria" and "security requirements" for DREs.

140. The Secretary has failed to adopt rules setting minimum "evaluation criteria" and minimum "security requirements" for the subject DREs.

141. Colorado Revised Statute § 1-5-617 and Election Rule 45.3.3 require the Secretary to make certification reports and qualification reports that document and verify the testing and certification process undertaken and completed by the Secretary for each of the Subject DREs.

142. On information and believe, the Secretary has not made the certification or qualification reports and findings required by Colorado law and the Secretary's own Election Rules.

143. Pursuant to Colorado's Uniform Declaratory Judgments Act, C.R.S. § 13-51-101 *et seq.*, and C.R.C.P. 57 and 106, Plaintiffs are entitled to and request a judicial determination and declaratory judgment that use of the Subject DREs certified by the Secretary—or any other DRE voting machine that does not fulfill the statutory requirements—violates Defendants' statutory duty to put in place voting machines that correctly record and accurately count the votes cast by Colorado voters.

144. In addition, Plaintiffs are entitled to a judicial determination and declaration that the Secretary has not fulfilled her statutory duties to establish minimum "evaluation criteria" and minimum "security requirements" for the Subject DREs, and has not complied with the statutory requirements and her own Election Rules in testing and certifying the Subject DREs.

145. Colorado Revised Statute § 1-5-615 further requires that an electronic voting system "saves and produces the records necessary to audit the operation of the electronic or electromechanical voting system, including a paper record with a manual audit capacity." *See also* 8 C.C.R. § 1505-1 (45).

146. The Subject DREs certified by the Secretary do not provide a durable, permanent paper record suitable for a manual audit.

147. Pursuant to Colorado's Uniform Declaratory Judgments Act and C.R.C.P. 57 and 106(a)(2), Plaintiffs are entitled to and request a judicial determination and declaratory judgment that use of the Subject DREs certified by the Secretary—or any other DRE voting machine that does not fulfill the statutory requirements—violates Defendants' statutory duty to put in place voting machines that produce an accurate, durable, permanent paper record that would allow Colorado to conduct an audit and recount.

148. Plaintiffs further request a judicial determination and declaration that the Secretary cannot certify the Subject DREs—or any other DRE voting machine that does not fulfill the statutory requirements—for use in any State election.

149. Plaintiffs further request a judicial determination and declaration that Defendants cannot use the Subject DREs—or any other DRE voting machine that does not fulfill the statutory requirements—in any State election.

**Second Claim for Relief**  
**(Declaratory Judgment—Violations of C.R.S. § 1-5-704 and 8 C.C.R. § 1505-1 (34 – 35))**

150. Plaintiffs incorporate the allegations set forth in the foregoing paragraphs of this Complaint as if fully set forth herein.

151. Pursuant to C.S.R. § 1-5-704 and C.E.R. 34 and 35, all new voting systems acquired by Colorado counties must be accessible to persons with disabilities and provide the voter with the same opportunity for access and participation as for other voters.

152. The Subject DREs certified by the Secretary do not allow many disabled voters to vote privately and independently as Colorado Statutes and Election Rules require.

153. Pursuant to Colorado's Uniform Declaratory Judgments Act and C.R.C.P. 57 and 106, Plaintiffs are entitled to and request a judicial determination and declaratory judgment that use of the Subject DREs certified by the Secretary—or any other DRE voting machine that does not fulfill the statutory requirements—violates Plaintiffs' statutory rights to voting systems that allow disabled voters to vote privately and independently, as required by Colorado law.

154. Plaintiffs further request a judicial determination and declaration that the Secretary cannot certify the Subject DREs—or any other DRE voting machine that does not fulfill Plaintiffs' statutory rights—for use in any state election.

155. Plaintiffs further request a judicial determination and declaration that Defendants cannot use the Subject DREs—or any other DRE voting machine that does not fulfill Plaintiffs' statutory rights—in any state election.

**Third Claim for Relief**  
**(Declaratory Judgment—Violations of Colo. Const. art. II, § 5)**

156. Plaintiffs incorporate the allegations set forth in the foregoing paragraphs of this Complaint as if fully set forth herein.

157. Article II, Section 5 of the Colorado Constitution requires that elections be “free and open” and that “no power, civil or military, shall at any time interfere to prevent the free exercise of the right of suffrage.”

158. The use of the Subject DREs certified by the Secretary violates Colorado voters' rights to “free and open” elections and to be free of interference of their right of suffrage because such Subject DREs are highly vulnerable to tampering, do not accurately count and record votes, and do not allow for proper auditing and recount of ballots.

159. Pursuant to Colorado's Uniform Declaratory Judgments Act and C.R.C.P. 57 and 106, Plaintiffs are entitled to and request a judicial determination and declaratory judgment that use of the Subject DREs certified by the Secretary—or any other DRE voting machine that does not fulfill the statutory requirements—violates Plaintiffs' constitutional rights to free and open elections, and to the free exercise of their right of suffrage.

160. Plaintiffs further request a judicial determination and declaration that the Secretary cannot certify the Subject DREs—or any other DRE voting machine that does not fulfill Plaintiffs' constitutional rights—for use in any state election.

161. Plaintiffs further request a judicial determination and declaration that Defendants cannot use the Subject DREs—or any other DRE voting machine that does not fulfill Plaintiffs' constitutional rights—in any state election.

**Fourth Claim for Relief  
(Declaratory Judgment—Violations of Colo. Const. art. II, § 25)**

162. Plaintiffs incorporate the allegations set forth in the foregoing paragraphs of this Complaint as if fully set forth herein.

163. Article II, Section 25 of the Colorado Constitution states, “No person shall be deprived of life, liberty or property, without due process of law.”

164. By requiring some voters to cast their votes on inaccurate, unreliable, and insecure voting machines, thereby placing those voters at far higher risk of not having their votes properly counted or weighted, Defendants are denying some Colorado voters due process and equal protection of the law. To require some voters to vote on such flawed and insecure systems as the Subject DREs while others vote on safer, more accurate systems would result in an unequal election and the unequal protection of Coloradoans’ rights to vote.

165. Pursuant to Colorado’s Uniform Declaratory Judgments Act and C.R.C.P. 57 and 106, Plaintiffs are entitled to and request a judicial determination and declaratory judgment that use of the Subject DREs certified by the Secretary—or any other DRE voting machine that does not fulfill the statutory requirements—violates Plaintiffs’ constitutional rights to due process of law.

166. Plaintiffs further request a judicial determination and declaration that the Secretary cannot certify the Subject DREs—or any other DRE voting machine that does not fulfill Plaintiffs’ constitutional rights—for use in any state election.

167. Plaintiffs further request a judicial determination and declaration that Defendants cannot use the Subject DREs—or any other DRE voting machine that does not fulfill Plaintiffs’ constitutional rights—in any state election.

**RELIEF REQUESTED**

Wherefore, Plaintiffs request the following relief:

1. A declaration that the Subject DREs certified by the Secretary do not comply with the Colorado Constitution and Colorado Statutes.
2. A preliminary and permanent injunction prohibiting the Secretary from certifying electronic voting systems that do not comply with Colorado’s statutory and constitutional provisions.
3. A preliminary and permanent injunction prohibiting Defendants from purchasing or leasing and using the Subject DREs, or any other DRE voting machine that does not fulfill the statutory and constitutional requirements, for any election in Colorado.

4. A preliminary and permanent injunction prohibiting Defendants from training their personnel and poll workers on the use and operation of the Subject DREs.

5. A preliminary and permanent injunction requiring Defendants to put in place voting systems that comply with Colorado's statutory and constitutional provisions.

6. An award of other and further relief for Plaintiffs as may be appropriate.

Pursuant to C.R.C.P. 38 and 57(m), Plaintiffs demand a trial by jury.

Dated: June 1, 2006

Respectfully submitted,

*Original signature on file at the law firm of Wheeler Trigg  
Kennedy LLP*

s/ Paul F. Hultin  
Paul F. Hultin

**Plaintiffs' Addresses:**

Myriah Sullivan Conroy  
2110 Floral Drive  
Boulder, CO 80304

Michael Melio  
8219 West 90th Place  
Westminster, CO 80021

Julieann Murphy Cross  
14430 Watkins Mile Road  
Brighton, CO 80603

Michael Neil  
2551 South High Street  
Denver, CO 80210

Rochelle D. Cohen, M.D.  
1849 South Xenia Court  
Denver, CO 80231

Wendy Norris  
1309 Maple Street  
Fort Collins, CO 80521

Kathy Dean  
50 South Dutch Valley Road  
Bennett, CO 80102

Daniel Pinto  
2862 Ash Street  
Denver, CO 80207

Tony Delcavo  
4697 Stone Canyon Ranch Road  
Castle Rock, CO 80104

Jeffrey A. Sherman  
1506 Redwing Lane  
Broomfield, CO 80020

Ann Goldstein  
1695 Orchard Avenue  
Boulder, CO 80304

Robert Soto  
3140 Quazar  
Durango, CO 81301

Timothy J. Chappell  
432 26th Avenue Court  
Greeley, CO 80634