



PUBLIC COMMENT M E M O R A N D U M

TO: Secretary of State Scott Gessler

FROM: Myriah Sullivan Conroy and Jeffrey A. Sherman

DATE: February 14, 2012

SUBJECT: Comments Regarding Notice of Proposed Rulemaking From the Office of the Secretary of State.

On January 13, 2012, Colorado Secretary of State Scott Gessler (the “Secretary”) issued a Notice of Proposed Rulemaking (the “Notice”) to discuss proposed changes to Colorado Election Rule 43. The Notice indicated that a public meeting will be held on February 14, 2012 from 1:00 p.m. to 5:00 p.m. Wheeler Trigg O’Donnell LLP (“WTO”) represents Myriah Sullivan Conroy and Jeffrey A. Sherman (the “Electors”) and hereby submits written comments as invited by Section V of the Notice of Proposed Rulemaking.

The purported purpose of the changes to the election rules is to “improve the administration and enforcement of Colorado elections law.” Notice, at p. 1 (citation omitted). However, Secretary Gessler is proposing to weaken or eliminate the court-ordered security protections that protect against the well-documented vulnerability of DREs to hacking and vote tampering. He offers no scientific or technical support for the proposed changes. Secretary Gessler is apparently willing to compromise the integrity of Colorado’s elections as a palliative to the county clerks for what he calls administrative efficiency. Colorado voters deserve more from their chief elections officer.¹

I. CONDITIONS OF USE PROBLEMS

The current Conditions of Use for DREs in Colorado have been in effect since 2008 and are an important part of the policies and procedures that protect against hacking of DREs and voter tampering that threatens the integrity of Colorado’s elections. The current Conditions of Use were created by a Testing Board of experts in DREs and were implemented under the Voting Systems Certification Program. Experts from around the nation contributed to the Testing Board’s work, and now the Secretary seeks to destroy the Testing Board’s work and to destroy the security measures currently in place for DREs in Colorado—and all of it is being done behind closed doors in violation of Colorado law.

¹ It appears that the Elector’s concerns expressed in their initial public comment memorandum dated December 8, 2011, were largely ignored by the Secretary.

February 14, 2012

Page 2

Secretary Gessler's November 9, 2011 Notice included a preliminary draft of "Revised Conditions of Use" for each of the four types of DREs currently in use in Colorado. Then, at the hearing on December 8, 2011, the Secretary distributed more specific proposed changes to the Conditions of Use for the four types of DREs currently in use in Colorado. As of November 9, 2011, clearly the Secretary's office believed that it was required by law to subject the proposed "Revised Conditions of Use" to public comment and a public hearing.

The Secretary's January 13, 2012 Notice does not contain a reference to Conditions of Use for DREs. But, at least two recent emails from the Secretary of State's staff indicate that the Secretary may believe he is entitled to unilaterally revise the Conditions of Use without the public's input and without a public hearing. First, Michael Hagihara of the Secretary of State's office told a concerned voter in an email that he does "not know whether a hearing will be held prior to this office issuing revised Conditions." See February 9, 2012 Email Fr. M. Hagihara to M. Eberle, Exhibit 1 hereto. Second, Judd Choate of the same office, stated that the Secretary of State's Office does not think that it is required to be abide by the Colorado Administrative Procedure Act when revising the DRE Conditions of Use:

Mr. Hultin: Are you contending that the Conditions of Use are not subject to the requirements of the Colorado Administrative Procedures Act?

Mr. Choate: I'm not "contending" anything. I am saying that we find no statutory requirement to provide a rulemaking process for conditions of use.

See February 9, 2012 Email Fr. J. Choate to P. Hultin, Exhibit 2 hereto. Such statements from the Secretary of State's Office run contrary to the law in Colorado, are an effort by the Secretary to diminish election security measures in violation of the law, and are plainly meant to undertake covert actions that threaten the integrity of Colorado's elections. Specifically, the Colorado Revised Statutes state as follows:

When any agency is required or permitted by law to make rules, in order to establish procedures and to accord interested persons an opportunity to participate therein, the provisions of this section shall be applicable.

C.R.S. § 24-4-103(1). That same section of the Colorado Revised Statutes requires notice of a proposed rule-making to be provided. C.R.S. § 24-4-103(3)(a). In addition, the Colorado Supreme Court explained in an instructive Administrative Procedures Act case that "In resolving this issue we are not bound by the label the PUC attached to its actions; rather, we must look at the substance of what the commission has actually done" to determine whether the agency was involved in Rule-Making as defined by C.R.S. § 24-4-102(16). *Home Builders Ass'n of Metropolitan Denver v. Public Utilities Comm'n*, 720 P.2d 552, 560 (Colo. 1986). The Court added that The Public Utilities Commission undertook Rule-making because the PUC's decision was "nothing less than an 'agency statement of general applicability and future effect implementing [and] declaring policy,' § 24-4-102(15), 10 C.R.S. (1982), and, under the

February 14, 2012

Page 3

particular circumstances present here, is functionally indistinguishable from *de facto* rule-making.” *Id.*

In fact, the current Conditions of Use state as follows:

The Testing Board recommends that the Secretary of State adopt the following conditions for use of the voting system. These conditions are required to be in place *should* the Secretary approve for certification any or all of the items indicated in the **COMPONENTS** section. The Testing Board has modified the conditions based on information provided through public hearing under legislative updates to consider additional procedures. Any deviation from the conditions provides significant weakness in the security, auditability, integrity and availability of the voting system.

See <http://www.sos.state.co.us/pubs/elections/VotingSystems/files/ESSCFU.pdf> (emphasis in original). The foregoing excerpt tells the entire story, yet Secretary Gessler is seeking to blatantly violate the law by changing the Conditions of Use behind closed doors. The Electors strongly disagree with any such action and such an action by the Secretary, behind closed doors and without public notice and comment violates the law and is an affront to transparent, free, and fair elections in Colorado.

II. HISTORICAL PERSPECTIVE ON DRES IN COLORADO

A. In 2006, the Denver District Court Ordered the Secretary of State’s Office to Establish New Requirements for Certification of DREs and to Adopt Stringent Security Procedures for the Use of DREs.

Conroy et al. v. Dennis, Case No. 06-CV-6072, Denver District Court (“*Conroy*”), marks the point in time when the Electors first became concerned about the dubious actions of the Secretary of State’s office regarding the security vulnerability and ease of hacking into DREs. In *Conroy*, the Electors, along with others, formed a group of non-partisan plaintiffs who sued then Secretary of State Ginette Dennis (“Dennis”) in her official capacity to require Dennis to comply with applicable law in certifying DREs for use in Colorado elections. See Opinion of the Denver District Court (the “Opinion”), Exhibit 3 hereto, at p. 1. After a three-day trial, the District Court ruled in favor of the Electors on a number of key issues.

Most importantly for purposes of these Public Comments, the proposed changes to Election Rule 43, and the proposed changes to the conditions of use for DREs, the District Court ordered as follows:

1. The Secretary was to promulgate a rule containing minimum security standards for DREs as required by C.R.S. § 1-5-616(1)(g).
2. The Secretary was to retest previously certified systems or any new systems, using the revised security standards to be promulgated by the Secretary, prior to

the next primary, general or statewide ballot issue election following the November 7, 2006 general election, whichever comes first.

3. Prior to the November 7, 2006 election, the Secretary was ordered to require county election officials to implement security standards governing the use of DREs. County security standards were required to be developed immediately with input and cooperation from Plaintiffs, and were ordered to be designed to reduce the significant risks of tampering, to increase the security relating to handling and use of DREs, and to provide for secure and proper handling and storage of the paper record of votes cast on DREs in a controlled environment.

See Opinion at pp. 7 – 8. The Opinion was not appealed and remains binding on the current Secretary. The county security standards and procedures were ordered because of overwhelming scientific evidence that the DREs are notoriously insecure and can be easily hacked and reprogrammed to change votes.

The retesting of the four existing DRE systems then in use in Colorado resulted in decertification of three of the four DRE systems. In light of the emergency created by this expected result, interim legislation was passed and stringent security procedures and conditions of use were developed by the Secretary of State to minimize the substantial risks associated with the use of these dubious DRE voting systems.

It is these 2008 security rules and conditions of use that the Secretary now proposes to relax or eliminate entirely. He offers no reason for this other than the self-serving and conclusory statement that he is “considering amendments to the elections rules in order to improve the administration and enforcement of Colorado elections law.” Notice at page 1 (citations omitted).

B. The Election Reform Commission

Following the ruling in *Conroy*, and as a result of Senate Bill 08-243, an 11-member Election Reform Commission was created. Secretary Gessler was a member of the Election Reform Commission, and Mr. Hultin was also a member. Following a series of meetings between November 2008 and February 2009, which included: (1) the taking of public testimony; (2) hearing presentations from experts and stakeholder representatives in the fields of elections and voting technology; and (3) deliberating on issues related to reform of Colorado’s election system and the use of DREs in Colorado, the Election Reform Commission created a Final Report. The Election Reform Commission’s Final Report was submitted to the members of the Colorado House and Senate State, Veterans, and Military Affairs Committees. *See* Final Report of the Election Reform Commission dated February 27, 2009, Exhibit 4 hereto.

Importantly, of the 20 recommendations the Election Reform Commission approved, numbers 7 and 8 relate directly to DRE security and auditing. *See* Final Report of the Election Reform Commission, Ex. 4, at pp. 5 – 7.

C. House Bill 09-1335 Becomes Law And Reforms Election Law In Colorado.

As a result of the Election Reform Commission's Final Report, the Sixty-Seventh General Assembly of the State of Colorado passed House Bill 09-1335 that was signed into law by Governor Bill Ritter, Jr. The provisions of House Bill 09-1335 are now found in the Colorado Election Code, C.R.S. s. 1-1-101 *et seq.* There were many critical and much-needed changes to Colorado's election laws in House Bill 09-1335, which included a prohibition on further purchases of DREs, the requirement of a paper record for votes cast on DREs, and the adoption of risk-based audits to mitigate the risk of election fraud that arises from the use of DREs. For all Coloradans who want fair, transparent, and secure elections, House Bill 1335 was a significant step forward.

III. ELECTRONIC VOTING IS WIDELY RECOGNIZED AS A DEFICIENT AND UNSECURE METHOD OF VOTING AND ANY CHANGES TO COLORADO ELECTION RULES SHOULD REQUIRE GREATER SECURITY, NOT WEAKER SECURITY POLICIES SUGGESTED BY THE PROPOSED CHANGES.

Electronic voting became much more prevalent following the passage of the federal law known as the Help America Vote Act of 2002 ("HAVA"), P.L. No. 107-252. However, in the massive expansion of electronic voting associated with HAVA, the development and widespread use of DREs resulted in the compromising of voting security that was widespread, and that became a matter of great public concern both in Colorado and throughout the entire country. Since *Conroy* and the passage of House Bill 09-1335 in 2009, computer scientists and security experts have continued to demonstrate the woeful lack of security in electronic voting.

For example, in one of the most egregious examples of voting security being easily compromised, national security experts from the Argonne National Laboratory, which is now part of the Department of Homeland Security, recently demonstrated how easy it was to make a "man in the middle" hack into a Diebold DRE.² Amazingly, the Argonne computer scientists and security experts demonstrated that it was easy to remotely hack into a Diebold DRE with materials that cost less than \$26.00. *See Researchers Hack Voting Machine for \$26*, Sept. 30, 2011, at <http://www.foxnews.com/scitech/2011/09/30/researchers-hack-voting-machine-for-26/>. The Diebold DREs are used in many counties in Colorado. Diebold's voting machine business is now owned by Dominion Voting Systems, a Denver-based company. *See id.* Over 22 states use Dominion Voting Systems' DREs. *Id.* The Argonne researchers were able to hack into the Diebold machines from up to a half-mile away and change a voter's vote immediately after the vote was cast. *Id.* A potential hacker could of course be a Republican, a Democrat, or a foreign

² A copy of the full Argonne National Laboratory report titled *Suggestions for Better Election Security From the Vulnerability Assessment Team at Argonne National Laboratory*, October 2011, is attached as Exhibit 5 hereto; *see also Diebold Voting Machines Can Be Hacked By Remote Control*, September 27, 2011, at <http://www.salon.com/2011/09/27/votinghack/>.

February 14, 2012

Page 6

person motivated to simply disrupt or destroy the accurate results in a given election. This is why the Argonne scientists consider DRE voting systems a national security risk.

Of note, Deibold's DRE unit was based in former Congressman Bob Ney's home state, the same Congressman who was convicted of felonies related to Jack Abramoff's lobbying activities and proposed amendments to the Help America Vote Act. *See Factual Basis for the Plea of Robert W. Ney*, at pp. 5 and 11, at <http://abcnews.go.com/images/Politics/pin.ney.fact.pdf>.

In another disturbing example of electronic vote hacking, the Washington D.C. Board of Elections and Ethics was forced to suspend an internet voting trial after the system was successfully hacked by a group of University of Michigan computer science students. *See Hacker Infiltration Ends D.C. Online Voting Trial*, October 7, 2011, at http://voices.washingtonpost.com/debonis/2010/10/hacker_infiltration_ends_dc_on.html. The online voting system was designed to allow military service members living abroad the opportunity to vote online. In fact, a member of the D.C. Board of Elections and Ethics invited would-be hackers to "give it your best shot," at hacking into the system. *See id.* The University of Michigan students did just that. The students hacked into the internet-based system and rigged the system such that after a voter cast his or her vote, the University of Michigan fight song, *The Victors*, immediately began playing for the voter. *See id.* While Colorado currently does not have online voting, long standing and widely documented threats to the primitive security of DRE electronic voting are real and problematic. As a result, states such as Colorado should be amending their election rules and conditions of use for DREs to make them more rigorous and tighter, not weakening and loosening them as Secretary Gessler proposes to do with his changes to Election Rule 43.³

³ A private California-based company named Everyone Counts that develops internet voting security systems for elections from Australia to Florida recently partnered with the Academy of Motion Picture Arts and Sciences to develop allegedly secure online voting for Academy members to vote on the Oscars. However, as David Dill, Professor of Computer Science at Stanford University explains, internet voting security is simply non-existent:

Everybody would like there to be secure internet voting, but some very smart people have looked at the problem and can't figure out how to do it. The problem arises as soon as you decouple the voter from the recorded vote. If someone casts a ballot for best actor A and the vote is recorded for best actor B, the voter has no way of knowing the ballot has been altered, and the auditor won't be able to see it either.

See Oscars Vote Vulnerable to Cyber Attack Under New Online System, Experts Warn, at <http://www.guardian.co.uk/film/2012/feb/02/oscars-vulnerable-cyber-attack-experts-warn>. If the same company that purports to sell safe and secure internet election software cannot even ensure that the Oscar voting is secure, the American voting public should not be asked to compromise American elections with internet voting systems that simply are not secure.

IV. THE PRELIMINARY DRAFT OF POTENTIAL REVISIONS TO ELECTION RULE 43 WILL MAKE COLORADO ELECTIONS LESS SECURE, LESS UNIFORM AND LESS TRANSPARENT TO THE POINT THAT THE PROPOSED CHANGES INVITE VOTING FRAUD.

A. Proposed Changes to Colorado's Election Rule 43

There are several major areas of responsibility and accountability that are absent from the proposed revisions to Election Rule 43 circulated by Secretary Gessler. These changes show a lack of concern for the integrity of the voting process, and if implemented, the revisions make it easier for hacking and vote tampering to go undetected. It has been conclusively established that DREs can be easily hacked and reprogrammed to change votes. Gessler does not deny or present any evidence to the contrary. He proposes to eliminate critical security protections for "improved administration and enforcement of Colorado elections law." This defies common sense, is arbitrary and capricious, and clearly violates the law.

Secretary Gessler's proposed rule ignores problems and risks that have been conclusively established in Court in Colorado and by prominent computer scientists during the last five years all over the United States.

With respect to the Notice itself, the ~~striketrough~~ method of altering section numbers and content is somewhat confusing. The Electors suggest that a "clean" version of the proposed changes to Election Rule 43 also be circulated with any proposed changes or amendments in the future so that Secretary Gessler's intended actions can be easily understood by all concerned voters.

1. Relaxed Physical Security Requirements

Both the current and proposed versions of the rule involve the use of serial-numbered, tamper-proof seals on DREs and other voting equipment. But the proposed version compromises how security is to be maintained using these seals.

First, the version proposed by Secretary Gessler states that "[i]f a seal is inaccessible and cannot be removed, then it is not necessary to verify that seal serial number." Proposed Changes, Section 43.2.2, p. 5. This cryptic instruction is likely to result in compromised security. Who decides that a seal is inaccessible and cannot be removed? County election officials or a creative hacker doing his best to beat the system? And if a numbered seal is not verified, then what is the purpose of even having it placed on the machine?

Second, in the current version of the rule, at least one seal is to be placed on all four sides of the seam connecting the two sides of the case containing the electronic components of the voting machine. Proposed Changes, Current Section 43.8.24(a)(iii), p. 6. In contrast, the proposed version requires that "[s]eals shall be used at either the seams of the case or at key entry points such as screw access points." Proposed Changes, at 43.2.2(A)(3), p. 6 (emphasis added). Rewriting the rule in this disjunctive and subjective way with no requirements regarding

mandatory requirements for placement of numbered seals, results in a significant decrease in security. For instance, what if seals are placed only over screw access points, but a hacker simply compromises the lock to open the case? If there are no seals on the seams, tampering would go undetected. This is contrary to the minimum standards published by the scientists and security experts for the Argonne National laboratory. See Exhibit 5 attached hereto.

Additionally, both versions of this rule only require these tamper-proof seals if the “firmware or software hash value” cannot be verified. The type of hacking recently demonstrated by the Argonne National Laboratory was accomplished remotely and was only detected because the hackers reported what they had done. It seems that even the current version of the rule does not offer adequate protection against remote, wireless hacking, which has recently been demonstrated. In light of the undisputed and widespread evidence (including evidence from computer scientists from Rice University and the University of Iowa presented in open court in the *Conroy* trial) that DREs are vulnerable to hacking, the Secretary should be focused on tightening the security measures in Rule 43, not loosening them.

Third, the current version of Rule 43 contains stringent security measures relating to which county employees can access the storage area for voting equipment and the mail-in ballot counting area. Proposed Changes, Current Section 43.8.3.3, p. 8. The proposed revision authorize a county to simply “request” from Secretary Gessler an “exemption” from all of the requirements in the event of “extreme circumstance.” Proposed Changes, Section 3.2.3(C)(2), p. 8. There is no explanation of what an “extreme circumstance” might be, and there is no reason given for providing the counties and the Secretary with the unfettered right to arbitrarily and capriciously declare that a so-called “extreme circumstance” exists, or how any concerned member of the public could be made aware that an exemption had been requested. This is a giant loophole, especially in light of Secretary Gessler’s track record on DREs.

2. *Relaxed Inspection Requirements*

Several of the proposed changes would eliminate important responsibilities of the Secretary with respect to monitoring the integrity of Colorado’s voting system.

The current version of Rule 43.8.6.1(e) states that “[t]he Secretary of State shall be required to inspect the counties’ maintenance records” for a set percentage of randomly-selected voting devices. Proposed Changes, Current Section 43.8.6.1(e), p. 11 (emphasis added). The proposed version eliminates the mandatory minimum percentage of voting devices that must be inspected and changes the language to “[t]he Secretary of State will annually inspect a county’s maintenance records on a randomly selected basis.” Proposed Changes, Section 3.2.6(E), p. 11 (emphasis added). The proposed wording arguably eliminates any meaningful volume of inspections by the Secretary, which is a clear signal to the counties that the current mandatory requirement, like much of Rule 43, has been relaxed, if not practically eliminated.

3. *Relaxed Reporting Requirements to the Secretary of State*

Beyond trying to reduce the Secretary's duty to inspect and ensure the integrity of the voting process, Secretary Gessler's proposed changes eliminate the security reporting that he would receive from the counties. There is no reason to eliminate this requirement.

For example, in the current version of the rule, Section 43.8.11.1, Remedies, requires that if an election judge notices that a seal has been broken or if there is a serial number discrepancy on the voting equipment, the judge is to immediately alert the County Clerk and then that person "shall investigate and report the incident to the Secretary of State...." Proposed Changes, Current Section 43.8.11.1, p. 17. The proposed revision eliminates the reporting of the potential security breach to the Secretary of State and instead the County Clerk must conduct an "internal investigation" and only if the County Clerk "is unable to determine why a seal was broken or why a discrepancy exists in a chain-of-custody log" must the clerk file an incident report with the Secretary. Proposed Changes, Section 3.2.11(A) and (B), p. 17. Therefore, if the County Clerk is notified of a broken seal, and learns that the machine was potentially hacked, he or she would not need to report that incident to the Secretary and instead would only need to conduct an internal investigation. This would leave discretion as to whether a security violation had occurred to the counties many of which do not have the resources, expertise or inclination to perform such an investigation. Any potential hacking incident would not be reported to a central location. This, of course, makes no sense and should not be any part of Rule 43 that is intended to prevent hacking and vote tampering.

Further, Rule 43 currently requires specific actions be taken if suspected tampering occurred before, during, or after the voting period. But in each of these sections the proposed changes, the requirement that a report be submitted to the Secretary is deleted. With no mandatory reporting or oversight, the use of highly vulnerable DREs is unsupervised and unchecked and any acts of local, systemic, or statewide fraud would easily go unreported and undetected. *See, e.g.* Current Section 43.8.11.3(2)(E) (which is deleted under the new Rule).

Additionally, in the current version of the rule, each county is required to submit a written report "addressing the existence or absence of any security issues related to the implementation and operation of the voting system" to the Secretary before that county can submit certified voting results. Proposed Changes, Current Section 43.8.11.4, p. 20. The proposed changes simply delete this provision. Like the other changes proposed, this is a blatant relaxation of provisions designed to protect against DRE tampering and election fraud in Colorado elections.

Under the current version of Rule 43, if serious equipment failure occurs, a polling place must contact the Secretary of State to obtain authorization for the use of provisional or mail-in ballots. Proposed Changes, Current Section 43.8.8.2, p. 14. If the proposed changes take effect, a polling place must simply notify the Secretary that they are going to use these replacement ballots—thus relieving the Secretary of any responsibility to investigate the serious equipment failure while leaving all decisions in the hands of the County Clerks who lack the resources and expertise to address issues of hacking and vote tampering in computerized voting systems. This change also diminishes a key source of state-wide data on the performance, or lack of

performance, of the dubious DREs because the County Clerk may never explain to the Secretary why the county is suddenly switching to provisional or mail-in ballots.

B. Deletion of Rule 27.8 Presents Significant Vote Counting Problems.

The Notice indicates that Election Rule 27.8 will be repealed. *See* Proposed Changes, at pp. 1 – 3. This is problematic because Rule 27.8 sets out specific time frames for submission and approval of alternative counting plans, whereas C.R.S. § 1-7-603 does not do so. Presumably, in deleting Rule 27.8, the Secretary is planning to simply rely on C.R.S. § 1-7-603, and if so, the Secretary should make this point clear at the public meeting on February 14, 2012.

V. CONCLUSION

Vote tampering and DRE hacking risks have increased, as proved by a group of scientists from the Nuclear Engineering Division of the Argonne National Laboratory. DRE technology that was substandard in 2006 has not kept pace with other advances in computer science and invasive technology. It is naive in the extreme to assume that there will be no games played with our elections. A hacker could be a Republican, a Democrat, a third party activist, a teenager having fun on election day, or a member of a terrorist group seeking to wreak havoc with a cornerstone of our democracy—the right to vote in a fair and democratic election.

In these uncertain technological times, and with DREs in use in Colorado until at least 2014, the Secretary should be strengthening Election Rule 43 and the conditions of use of dubious DRE voting systems. The Secretary should be taking on more responsibility for overseeing free, fair, secure, and safe elections in Colorado, not less. The proposed changes to Election Rule 43 should be immediately discarded and any future proposed changes should bolster DRE and overall election security, not diminish it. In addition, the Secretary must not violate the law and unilaterally and secretly change the Conditions of Use without public input and without a public hearing.

Exhibit 1

Johnson, Matt

Subject: FW: RE: Rule 43 hearing: Conditions for Use

----- Original Message -----

Subject: RE: Rule 43 hearing: Conditions for Use

Date: Thu, 9 Feb 2012 17:13:27 +0000

From: Michael Hagihara <Michael.Hagihara@SOS.STATE.CO.US>

To: 'Mary Eberle' <m.eberle@wordrite.com>

CC: Andrea Gyger <Andrea.Gyger@SOS.STATE.CO.US>, Judd Choate
<Judd.Choate@SOS.STATE.CO.US>

Ms. Eberle,

The current Conditions for Use will apply until this office issues revised Conditions. I do not know whether a hearing will be held prior to this office issuing revised Conditions.

Sincerely,

Michael Hagihara

Michael Hagihara
Voter Registration and Elections Management Manager
Colorado Department of State
1700 Broadway, Ste. 200
Denver, CO 80290
p: 303-894-2200 ext 6331
f: 303-869-4861

From: Mary Eberle [<mailto:m.eberle@wordrite.com>]

Sent: Thursday, February 09, 2012 10:04 AM

To: Michael Hagihara

Cc: Andrea Gyger; Judd Choate

Subject: Re: Rule 43 hearing: Conditions for Use

Dear Mr. Hagihara,

Thank you for this information. If I understand you correctly, the current Conditions for Use will apply until a hearing is held to revise them. Please confirm that impression, just for the record.

Sincerely,

Mary

Mary C. Eberle
1520 Cress Court
Boulder, CO 80304
(303) 442-2164

On 2/9/2012 9:47 AM, Michael Hagihara wrote:

Dear Ms. Eberle:

Andrea Gyger asked that I respond to the email that you sent her on February 5. We are waiting for the outcome of the Rule 43 rulemaking before we decide how to move forward with the Conditions for Use. If we decide to hold another meeting regarding the Conditions for Use our communications team will inform the public of the time and place for that meeting.

Sincerely,

Michael Hagihara

Michael Hagihara
Voter Registration and Elections Management Manager
Colorado Department of State
1700 Broadway, Ste. 200
Denver, CO 80290
p: 303-894-2200 ext 6331
f: 303-869-4861

From: Mary Eberle [<mailto:m.eberle@wordrite.com>]
Sent: Sunday, February 05, 2012 9:53 PM
To: Andrea Gyger
Subject: Re: Rule 43 hearing: Conditions for Use

Hi Andrea,

By what process will the current conditions for use be modified (if they are modified)? Will there be a hearing?

Thank you,
Mary

On 1/30/2012 1:48 PM, Andrea Gyger wrote:
Hi Mary,

The rule would apply to effective conditions for use. Until new conditions for use are released, the rule, if adopted, would apply to the current conditions for use. If new conditions are adopted the rule would then apply to those.

Thanks,
Andrea

From: Mary Eberle [<mailto:m.eberle@wordrite.com>]
Sent: Monday, January 30, 2012 1:39 PM
To: Andrea Gyger
Subject: Re: Rule 43 hearing: Conditions for Use

Good afternoon to you also, Andrea,

The information and links you sent are very helpful. Now I need a little more detail. Does the line 28 (copied below in red and blue) refer to the current conditions of use or the possible revised conditions of use discussed

on December 8, 2011?

Thank you,
Mary

On 1/30/2012 1:28 PM, Andrea Gyger wrote:
Good afternoon Ms. Eberle,

Thank you for your email. "Conditions for use" means the conditions that a voting system vendor with certified voting equipment in Colorado is required to meet. The current conditions are posted online at www.sos.state.co.us/pubs/elections/VotingSystems/CondsForUse.html. If new/amended rules are adopted, our office anticipates release of revised and updated conditions for use as well. A copy of the possible revised conditions for use that were discussed at the December 8, 2011 public meeting are available online at www.sos.state.co.us/pubs/rule_making/publicMeetings/2011/20111208Elections.html.

I hope this information helps. If you have additional questions or would like to submit written comments concerning the proposed election rules, please let me know.

Thanks,
Andrea

From: Mary Eberle [<mailto:m.eberle@wordrite.com>]
Sent: Saturday, January 28, 2012 1:10 PM
To: Andrea Gyger
Cc: Mary Eberle
Subject: Rule 43 hearing: Conditions for Use

Dear Andrea,

>From your email of January 13, 2012:

The following information is also available online at the Secretary of State's website:

- Rules and Notices of Rulemaking: www.sos.state.co.us/pubs/rule_making/rules.html
- Information relating to 2/14/12 rulemaking hearing: www.sos.state.co.us/pubs/rule_making/hearings/2012/RulesHearing20120214.html

Page 22 from 20120113_Elections_NoticeProposedRulemaking.pdf:

27 Affirm that the use of the certified voting equipment shall be conducted
28 in accordance with Rule 43 and the specific conditions for use of the
29 certified voting equipment; and

So, could you please tell me what conditions for use is meant?

Thank you,
Mary

Mary C. Eberle
1520 Cress Court
Boulder, CO 80304
(303) 442-2164

Exhibit 2

Johnson, Matt

Subject: FW: Notice of Public Meeting re ER 43 and Conditions of Use for certified voting equipment

From: Judd Choate [mailto:Judd.Choate@SOS.STATE.CO.US]
Sent: Thursday, February 09, 2012 4:22 PM
To: Hultin, Paul
Cc: Michael Hagihara; Andrea Gyger; Wayne Munster; Johnson, Matt
Subject: RE: Notice of Public Meeting re ER 43 and Conditions of Use for certified voting equipment

I'm not "contending" anything. I am saying that we find no statutory requirement to provide a rulemaking process for conditions of use.

Judd

From: Hultin, Paul [mailto:hultin@wtotrial.com]
Sent: Thursday, February 09, 2012 4:17 PM
To: Judd Choate
Cc: Michael Hagihara; Andrea Gyger; Wayne Munster; Johnson, Matt
Subject: RE: Notice of Public Meeting re ER 43 and Conditions of Use for certified voting equipment

Hi Judd,

Are you contending that the Conditions of Use are not subject to the requirements of the Colorado Administrative Procedures Act? Would you please copy Matt Johnson on all future communications.

Thanks,

Paul

Paul Hultin
Wheeler Trigg O'Donnell LLP
1801 California St.
Suite #3600
Denver, Colorado 80202
303-244-1840 (Direct)
303-929-1060 (Mobile)
303-244-1879 (Fax)

From: Judd Choate [mailto:Judd.Choate@SOS.STATE.CO.US]
Sent: Thursday, February 09, 2012 3:50 PM
To: Hultin, Paul
Cc: Michael Hagihara; Andrea Gyger; Wayne Munster
Subject: RE: Notice of Public Meeting re ER 43 and Conditions of Use for certified voting equipment

Hi Paul. We are not familiar with the "published as required by law" requirement that you mention. Could you please direct us to the statutory basis for this "requirement" for conditions of use?

Thanks, Judd

Judd Choate, Ph.D., J.D.
Director, Division of Elections
Colorado Department of State
1700 Broadway Suite 200
Denver, CO 80290
Office - 303-894-2200
judd.choate@sos.state.co.us

From: Hultin, Paul [<mailto:hultin@wtotrial.com>]
Sent: Thursday, February 09, 2012 1:27 PM
To: Andrea Gyger
Cc: Johnson, Matt; DRE - Sherman, Jeff; Myriah Conroy; Wayne Munster; Michael Hagihara
Subject: RE: Notice of Public Meeting re ER 43 and Conditions of Use for certified voting equipment

Dear Andrea,

Thanks for your response. Actually the conditions of use were handed out at the December 8 hearing and to my knowledge have not been published as required by law. I am informed that your office is contending that Secretary Gessler may change those by fiat. If I am wrong about this please advise.

Thanks

Paul Hultin
Wheeler Trigg O'Donnell LLP
1801 California St.
Suite #3600
Denver, Colorado 80202
303-244-1840 (Direct)
303-929-1060 (Mobile)
303-244-1879 (Fax)

From: Andrea Gyger [<mailto:Andrea.Gyger@SOS.STATE.CO.US>]
Sent: Thursday, February 09, 2012 12:02 PM
To: Hultin, Paul
Cc: Johnson, Matt; DRE - Sherman, Jeff; Myriah Conroy; Wayne Munster; Michael Hagihara
Subject: RE: Notice of Public Meeting re ER 43 and Conditions of Use for certified voting equipment

Good afternoon Mr. Hultin,

Thank you for your email. The notice of public meeting, released on 11/9/11, includes a copy of the proposed Conditions for Use considered on 12/8/11. A copy is available online at www.sos.state.co.us/pubs/rule_making/publicMeetings/2011/20111208Elections.html. We are not proposing any changes to the Conditions of Use at this time. The current conditions are available online at www.sos.state.co.us/pubs/elections/VotingSystems/CondsForUse.html.

The February 14th hearing is a formal rulemaking hearing regarding proposed amendments to the Election Rules concerning county security procedures. A copy of the notice and related documents are available at www.sos.state.co.us/pubs/rule_making/hearings/2012/RulesHearing20120214.html. The Conditions for Use are not codified in rule, therefore we are not scheduled to discuss any proposed modifications during the rulemaking hearing.

I hope this information helps. If you have any additional questions or would like to submit written comment regarding the proposed rules, please let me know.

Thank you,
Andrea

From: Hultin, Paul [<mailto:hultin@wtotrial.com>]
Sent: Tuesday, February 07, 2012 7:22 AM
To: Andrea Gyger
Cc: Johnson, Matt; DRE - Sherman, Jeff; Myriah Conroy
Subject: RE: Notice of Public Meeting re ER 43 and Conditions of Use for certified voting equipment
Importance: High

Hi Andrea,

I just checked the web page and did not find the proposed changes in conditions of use for the 1/14 public hearing. I apologize if I missed them

They were not posted before the 12/8 hearing and I do not see them now. Can you send Matt and me the link to the proposed conditions of use or can you please send us a PDF with what was handed out on 12/8 and any changes since then.

Thanks,

Paul

Paul Hultin
Wheeler Trigg O'Donnell LLP
1801 California St.
Suite #3600
Denver, Colorado 80202
303-244-1840 (Direct)
303-929-1060 (Mobile)
303-244-1879 (Fax)

Exhibit 3

<p>DISTRICT COURT, CITY AND COUNTY OF DENVER, COLORADO</p> <p>1437 Bannock Street Denver, CO 80202</p> <hr/> <p>MYRIAH SULLIVAN CONROY, ET AL.,</p> <p>Plaintiffs,</p> <p>v.</p> <p>GINETTE DENNIS, IN HER OFFICIAL CAPACITY AS COLORADO SECRETARY OF STATE ,</p> <p>Defendant.</p>	<p style="text-align: center;">▲ COURT USE ONLY ▲</p>
	<p>Case No.: 06 CV 6072</p> <p style="text-align: center;">Ctrm.: 1</p>
<p>FINDINGS OF FACT AND CONCLUSIONS OF LAW</p>	

THIS MATTER came before the court for trial from September 20, 2006 to September 22, 2006. Plaintiffs' Complaint alleges, *inter alia*, that the Secretary of State failed to properly certify voting systems approved for use in Colorado. Upon consideration of the record and evidence presented at trial, the court makes the following findings of fact and conclusions of law.

FINDINGS OF FACT

1. The Plaintiffs in this case are Colorado electors.
2. Defendant Ginette Dennis is the Colorado Secretary of State (hereinafter "Secretary"). The Secretary is responsible for supervising "the conduct of primary general, congressional vacancy, and statewide ballot issue elections" in Colorado. § 1-1-107 (1)(a), C.R.S. (2006).
3. The Colorado General Assembly has authorized the use of direct recording electronic voting systems ("DREs"). A DRE is "a device by which votes are recorded electronically, including a touchscreen system." § 1-1-104(14.5), C.R.S. (2006).
4. Colorado law requires that DREs comply with federal standards, C.R.S. § 1-5-608.2, that DREs be qualified by an independent testing authority, C.R.S. § 1-5-608.5, and that DREs be certified by the Secretary, C.R.S. § 1-5-614. Additionally, counties must implement security requirements at the local level that are approved by the Secretary.

5. Under § 1-5-616(1), C.R.S. (2006), the Secretary is required to adopt rules “that establish minimum standards for electronic and electromechanical systems regarding: (a) Functional requirements; (b) Performance levels; (c) Physical and design characteristics; (d) Documentation requirements; (e) Evaluation criteria; (f) Audit capacity; (g) Security requirements; (h) Telecommunications requirements; and (i) Accessibility.

6. Pursuant to her duties under § 1-5-616, the Secretary adopted Election Rule 45, 8 CCR 1505. Rule 45 was promulgated as an emergency rule on October 3, 2005. The emergency adoption of Rule 45 was driven by internal delays within the Secretary’s office in drafting the rule.

7. Under § 1-5-617(2), C.R.S. (2006), the Secretary must “appoint one or more experts in the fields of data processing, mechanical engineering, or public administration to assist in the examination and testing of electronic or electromechanical voting systems submitted for certification and to produce a written report on each system.”

8. Len Vest was initially appointed as the Secretary’s expert and was in charge of promulgation of the rules establishing minimum standards for DREs. John Gardner was appointed to work with and assist Vest. Mr. Vest resigned in the fall of 2005.

9. When Vest resigned in the fall of 2005, the Secretary appointed Gardner to assume Vest’s responsibilities. Gardner became the appointed expert under § 1-5-617(2). Gardner took over the responsibility of promulgating minimum standards under C.R.S. § 1-5-616(1), and was put in charge of DRE examination, testing, and certification. There is no evidence that the Secretary or Deputy Secretary reviewed Gardner’s qualifications when asking him to assume Vest’s duties.

10. Gardner has a degree in architecture. He does not have a degree in data processing, mechanical engineering or public administration, although he does have some data processing experience as an IT manager in El Paso County, and he has some public administration experience working at the El Paso County Clerk and Recorder’s Office as well as at the Secretary of State’s office. He has no formal academic training in computer science or computer security. During his four years in the El Paso County Clerk and Recorder’s office, Gardner was responsible for election tabulation equipment. He coordinated and planned the programming, ballot order, training and deployment of all equipment related to conducting elections for El Paso County.

11. Prior to submitting an electronic or electromechanical voting system to the Secretary for certification, a vendor must be qualified by an independent testing authority approved by the Federal Election Commission. § 1-5-608.5, C.R.S. (2006). Upon receiving approval by an independent testing authority (“ITA”), a vendor may submit its system to the Secretary for certification. § 1-5-617(1)(a), C.R.S. (2006). The Secretary must examine each system and

determine whether the system complies with statutory requirements set forth in § 1-5-615, C.R.S. (2006), as well as the standards established by the Secretary under § 1-5-616, C.R.S. (2006). See § 1-5-617(1)(b), C.R.S. (2006).

12. The Secretary argued that she relied in large part on federal ITA testing to establish the security of the DREs. However, the evidence established that the ITA testing was deficient in a number of areas. For example, reports of ITA testing reveal that certain DREs were not subjected to software security tests that would reveal the software's vulnerability to malicious software attacks or tampering by telecommunication or data transmission.

13. Four vendors submitted their systems for certification in late 2005. These vendors are Diebold, Sequoia, Hart Intercivic, and ES&S.

14. The certification process did not commence until late in 2005. The Secretary's staff was under extreme time pressure because, to comply with federal law requirements, the certification process had to be completed in time to have the DREs in place for the August 2006 primary. Additionally, there was political pressure from counties for the Secretary's office to complete the certification process quickly. Some counties, particularly Mesa County, faced economic pressure because they had invested large sums of money in reliance on the assumption that the machines would be certified. In the face of this pressure, the Secretary's staff took unusual and extraordinary measures to push the DREs through the certification process.

15. Most of the testing conducted by the Secretary on the electronic voting systems is functional. That is, the Secretary's certification simply confirms that the voting system presented to the State is the same as the one qualified at the federal level, and tests to determine that the system can perform state-specific requirements. The security requirements for the electronic voting systems are contained in Rule 45.5.2.6. These requirements consist primarily of a requirement that vendors submit certain documentation. There is no evidence that any of the required documentation was ever reviewed, analyzed, or evaluated by the Secretary's office.

16. The Secretary is required to determine whether each voting system disallows unauthorized changes to system capabilities for certain operational functions, including defining ballot formats, casting and recording votes, and calculating vote totals consistent with defined ballot formats. John Gardner testified that he checked the DREs for compliance with this requirement during the certification process. Gardner's functional tests did not measure potential flaws in computer codes, nor did he test the robustness of the programming or the vulnerability of the programming to unauthorized tampering, except in cursory fashion.

17. By rule, the Secretary is required to compile a log of the testing procedures for each voting system. Among other things, the log must include a test description, notes of test, operating steps and deviations from requirements. Rules 45.6.2.2.3, 45.6.2.2.4 and 45.6.2.2.5. The Secretary's test logs do not identify the tests that were actually performed or the

methodologies used. The logs essentially disclose only whether a particular piece of equipment passed or failed.

18. The DREs must meet the accessibility requirements established in § 1-5-704, C.R.S. (2006). There is evidence that some of the DREs do not meet all of these requirements. For example, C.R.S. § 1-5-704(d) requires that a DRE play audio and video simultaneously; the ES&S system was certified despite the fact that it does not meet this requirement. However, Colorado voters with disabilities testified that even the noncompliant DREs provide an opportunity to vote independently and with more privacy than is available with traditional paper ballot systems.

19. The Secretary certified the systems presented by the four vendors. The Secretary imposed conditions on some of the certifications.

20. The DREs were used in the primary election held on August 8, 2006. There is no evidence of any actual or attempted security breaches or tampering during that election. There is no evidence that the DREs malfunctioned in any way that improperly or inaccurately recorded or tabulated votes.

21. Pursuant to the Secretary's Election Rule 43.7.1, each county must file with the Secretary security procedures for the

physical security of election equipment, software and firmware, election materials, polling places and counting centers, and equipment storage locations, including but not limited to (a) Locking mechanisms and seals; (b) Individuals with access to keys, door codes, vault combinations; (c) Temperature control (if necessary); (d) Security cameras or other surveillance; (e) Equipment maintenance procedures (See rule 11); (f) Transportation of equipment, ballot boxes, and ballots on election day; (g) Emergency contingency plans for equipment and polling places; (h) Any other procedures used to maintain physical security; (i) Internal controls for the voting system including software and hardware access controls and password management; and (j) Security Training for election judges.

22. Some of the written plans submitted by the counties for the August 2006 primary election and approved by the Secretary did not meet these requirements.

CONCLUSIONS OF LAW

1. The Court has jurisdiction pursuant to § 1-1-113, C.R.S. (2006). The Court may review activities of the Secretary under the Election Code to determine whether she "has committed or is about to commit a breach or neglect of duty or other wrongful act." § 1-1-

113(1), C.R.S. (2006). The Court may order the Secretary to substantially comply with the provisions of the code if the Court finds that the Secretary has breached a duty established under the Election Code.

2. In analyzing whether the Secretary has substantially complied with the Election Code, the Court must, at a minimum, consider the following factors: (1) the extent of noncompliance, that is a court should distinguish between isolated examples of district oversight and what is properly viewed as systematic disregard of the requirements under the Election Code, (2) the purpose of the provision violated and whether that purpose is substantially achieved despite the noncompliance, and (3) whether it can reasonably be inferred that the district made a good faith effort to comply. *Bickel v. City of Boulder*, 885 P.2d 215, 227 (Colo. 1994).

3. The Court also recognizes that it reviews the Secretary's actions subject to a deferential standard. When reviewing the Secretary's promulgation of rules, the Court will not substitute its judgment for that of the Secretary, but must determine whether the Secretary has acted in an unconstitutional manner, exceeded her statutory authority or otherwise acted in a manner contrary to statutory requirements. *Colorado Ground Water Commission v. Eagle Peak Farms, Ltd.*, 919 P.2d 212, 217 (Colo. 1996); *Citizens for Free Enterprise v. Department of Revenue*, 649 P.2d 1054, 1065 (Colo. 1982). This Court will not substitute its opinion or judgment for that of Secretary nor interfere with the Secretary's exercise of discretion based on evidence from which reasonable persons may draw different conclusions. *McQuate v. City of Boulder Fermented Malt Beverage Licensing Authority*, 420 P.2d 823, 824 (Colo. 1966). It is the court's duty, however, to determine whether the Secretary failed to comply with the law or to meet her statutory obligations, and where appropriate, to order the Secretary to comply.

4. Plaintiffs allege that the Secretary violated § 1-5-617(2), C.R.S. (2006), which provides, "The secretary of state shall appoint one or more experts in the fields of data processing, mechanical engineering, or public administration to assist in the examination and testing of electronic or electromechanical voting systems submitted for certification and to produce a written report on each system." Plaintiffs assert that Gardner was not an expert because he does not have a degree or formal training in any of the three fields listed under § 1-5-617(2) and, in particular, that he does not have expertise in computer science, programming, or computer security that would enable him to competently evaluate the potential vulnerabilities of the DREs. The Court certainly agrees that it would have been preferable for the Secretary to appoint a person with sufficient computer science skills to vigorously test the DREs for potential flaws and vulnerabilities. However, the statute affords the Secretary broad discretion. The statute does not establish a minimum level of training or experience. For example, the statute would allow the Secretary to appoint a person with a master's degree in public administration who had no computer or elections experience. The Court will not second-guess the Secretary's personnel decisions in the face of such a vague statutory mandate. Therefore, the Court is unable to conclude that the Secretary violated § 1-5-617(2).

5. Plaintiffs next contend that the Secretary did not establish minimum security standards. The Court agrees. Pursuant to § 1-5-616(1), the Secretary “shall adopt rules in accordance with article 4 of title 24, C.R.S., that establish minimum standards for electronic and electromechanical voting systems regarding...(g) Security requirements....” Rule 45.5.2.6.1 states that the vendor

shall provide documentation detailing voting system security in the areas listed below. At no time shall the system allow for unauthorized changes to system capabilities for: (a) Defining ballot formats; (b) casting and recording votes; (c) Calculating vote totals consistent with defined ballot formats; (d) Reporting vote totals; (e) Alteration of voting system audit records; (f) Changing, or preventing the recording of, a vote; (g) Introducing data for a vote not cast by a registered voter; (h) Changing calculated vote totals; (g) Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals; and (j) Preventing access to voter identification data and data cast by the voter such that an individual can determine the content of specific votes cast by the voter.

The Secretary contends that the factors listed in (a)-(j) of the rule constitute standards. However, a fair reading of the rule as a whole leads to the conclusion that those are functional requirements, not security standards. The rule primarily requires the vendor to provide documentation and does not require that anyone test, analyze, or even read the documentation. Supplying documentation is not a standard. While the rule states that systems shall not be subject to unauthorized changes, it does not set forth any security measures or prescribe any testing protocols that are designed to ensure that result. The lack of adequate security standards was highlighted by evidence introduced by Plaintiffs that showed certain DREs are vulnerable to tampering and reprogramming, yet those vulnerabilities were neither recognized nor addressed by any security measures. The Court concludes that the Secretary has not established minimum security requirements as mandated by § 1-5-616(1)(g), C.R.S. (2006), and did not adequately test the DRE systems against those minimum security requirements.

6. Plaintiffs next argue that the Secretary failed to maintain test logs in accordance with Rule 45.5.6.2. The test logs clearly do not meet the standards employed by the scientific community. The logs are grossly deficient in documenting what, if any, testing procedures were used and what standards were employed. They are inadequate to permit any person to repeat or verify the test procedures. However, test logs are not required by statute. The standards employed by the scientific community are not required by rule. Therefore, although the Secretary failed to even minimally document the tests that were the basis for certification, the court is unable to conclude that the Secretary failed to substantially comply with the applicable statutes and rules for certification.

7. Plaintiffs assert that the certification process was unduly influenced by political, economic, and time pressures. Elected officials do not operate in a vacuum. Citizens have a constitutional right to petition their elected officials. There are always political, economic, and

time pressures on elected officials. At some point these factors may loom large enough to render a decision arbitrary and capricious. In this case, there is insufficient evidence to establish that the Secretary's decisions to certify the DREs were based primarily on political pressure, and the court, therefore, declines to find the Secretary's actions to be arbitrary and capricious.

8. Plaintiffs contend that the voter-verified paper audit trail ("VVPAT") is subject to degradation and may not last for at least twenty-five months, as required by § 1-7-802, C.R.S. (2006). There was evidence that the thermal paper used by certain DREs can degrade over time and that it may degrade rapidly if exposed to light, heat, and humidity. While the Secretary has failed to demonstrate that the paper trail will last at least 25 months, the plaintiffs have not established that the paper trail will not, under controlled circumstances, last at least 25 months. Common sense dictates that at a minimum, the environment in which the VVPATs are stored should be controlled to minimize the risk of degradation. Therefore, the court orders the Secretary to immediately implement standards at the county level which shall assure the secure handling and storage of the VVPATs in a controlled environment.

9. Plaintiffs assert that the DREs do not strictly meet all of the requirements for accessibility by persons with disabilities. However, the evidence established that in most cases the DREs provide better access for persons with disabilities than paper ballots or other alternatives. Though the DREs may not meet every requirement for access to persons with disabilities, the remedy of decertifying the machines would have the effect of making it more difficult for persons with disabilities to vote. Obviously, such a remedy is inappropriate as it causes more harm than it ameliorates. The court, therefore, is unable to conclude that the DREs do not substantially comply with the applicable accessibility requirements.

10. Each county is required to file security plans with the Secretary. § 1-5-616(5), C.R.S. (2006). Each plan must meet the requirements set forth in Rule 43.7. Rule 43.1, 8 CCR 1505-1. The Secretary did not carefully evaluate the county security plans and in some cases approved plans that do not substantially comply with the minimum requirements of Rule 43.7. In addition, the Secretary has failed to adequately require all counties to provide appropriate minimum security at the county level. On-site security is particularly important in light of the Secretary's failure to adequately evaluate or test the DREs for security vulnerabilities.

11. Plaintiffs have requested, as a remedy, that the DREs be decertified. The court finds that decertifying the machines only six weeks before the elections would create more problems than it solves, and is therefore an inappropriate remedy.

Based on the foregoing findings of fact and conclusions of law, the Court hereby orders as follows:

1. The Secretary is ordered to promulgate a rule containing minimum security standards for DREs as required by § 1-5-616 (1)(g), C.R.S. (2006). (At trial, certain other portions of Rule 45 were shown to be far from ideal. The court cannot order the Secretary to promulgate a better


rule simply because a better rule could have been promulgated. Nonetheless, inasmuch as the rule must be amended anyway, the Secretary is encouraged to consider addressing other shortcomings of the rule.)

2. The Secretary is ordered to retest previously certified systems or any new systems, using the revised security standards to be promulgated by the Secretary, prior to the next primary, general or statewide ballot issue election following the November 7, 2006 general election, whichever comes first.

3. Prior to the November 7, 2006 election, the Secretary shall require county election officials to implement minimum security standards for that election. Such local standards shall be developed forthwith with input and cooperation from Plaintiffs, and shall be designed to reduce the possibility of tampering, to increase the security relating to handling and use of DREs, and to provide for secure and proper handling and storage of the VVPATs in a controlled environment.

Dated this 19th day of October, 2006, *nunc pro tunc*, September 22, 2006.

BY THE COURT,



Lawrence A. Mahzanares
District Court Judge

Exhibit 4

.....*from the desk of Ken Gordon, Chairman, Election Reform Commission*

February 27, 2009

Dear Members of the State, Veterans, and Military Affairs Committees:

Senate Bill 08-243 established the Election Reform Commission (ERC) with members chosen by the Speaker of the House, the President of the Senate, the Minority Leaders in the House and the Senate, the Secretary of State, and the Governor. The members of the ERC served without compensation or reimbursement for expenses. The legislation required that this report be presented to the House and Senate State Affairs Committees by March 1, 2009.

One could point to a number of events that led to the creation of the Election Reform Commission, but a logical starting point is to go back to the case of *Conroy v. Dennis* that went to trial in Denver District Court shortly before the 2006 election.

The plaintiffs in that case alleged that Secretary of State Gigi Dennis had not followed Colorado law in testing and certifying direct record electronic (DRE) voting machines. The Court found that the plaintiff's case had merit but was unwilling to decertify machines that Colorado's county clerks were relying on shortly before a general election. However, Judge Manzanares ordered the new Secretary of State, who turned out to be Mike Coffman, to establish standards and retest the machines following the 2006 election.

Pursuant to the new standards and testing, Secretary of State Coffman announced on December 17, 2007, that he was decertifying three of the four electronic voting systems used in Colorado, a decision that left over 50 Colorado counties without voting systems that they could use in the 2008 presidential election.

Multiple solutions to this predicament were proposed and debated during the 2008 legislative session. These included running a state-wide mail ballot election, using paper ballots, and giving the Secretary of State interim authority to certify the electronic voting machines for the 2008 general election.

Primarily because the county clerks maintained that they could not implement any other solution in the time frame required, the legislature passed House Bill 08-1155, which gave the Secretary of State interim discretionary authority which he used to recertify the decertified equipment. Since HB 08-1155 was a stop-gap solution to allow Colorado to be able to run a 2008 general election that was expected to, and in fact did, have the highest number of votes cast in Colorado's history, the legislation only allowed the electronic voting systems which had been decertified on December 17, 2007, to be used in the 2008 election. The bill sunsets on June 30, 2009. Therefore, over 50 Colorado counties are again facing elections without certified electronic voting machines and the Secretary of State is facing a number of legal and regulatory problems in dealing with certification of the systems that his predecessor had decertified in December of 2007, and which will again lose their certified status on July 1, 2009.

Since trying to pass election reform legislation during a general election year had proved problematic, the ERC was created to meet following the 2008 election in order to recommend changes in election laws and practices to be considered by the 2009 General Assembly.

In doing our work, the Commission divided itself into three subcommittees, Technology and Auditing, Uniformity and Simplification, and Registration and Database. Our recommendations therefore fall into these three categories.

Probably the most significant recommendation, and the one likely to receive the most attention, was our solution to the problem of electronic voting machine certification posed by the sunset of HB 08-1155. The recommendation by the Technology and Auditing Subcommittee reflected a balancing of interests. Greater detail is included within the body of this report, but the essence of the recommendation is that Colorado's counties will be allowed to use the electronic voting machines that they own through the year 2013. Following the year 2013, elections in Colorado will be conducted primarily on paper ballots counted by optical scan devices.

Paper ballots will provide an accessible, transparent, and verifiable method of conducting an election and the existence of the ballots will allow for reliable audits. It was not lost on the majority of the ERC that if nothing was done, these decertified, recertified machines could not be used after June 30, 2009, and if our recommendation is followed, Colorado's counties will have the best part of five years to implement a new election method.

It is also worthy of note that in the 2008 election, at least 70 percent of Coloradans voted on paper ballots either by mail or at polling places.

Commissioners Balink, Baisley, and Gessler dissented from this recommendation.

Extremely useful work was done by the Uniformity and Simplification and Registration and Database subcommittees as well.

The Registration and Database Subcommittee addressed issues relating to the Statewide Colorado Registration and Election System (SCORE), recommended clarifying the form used for voter registration, and recommended citizens present photo identification when registering to vote.

Significant recommendations by the Uniformity and Simplification Subcommittee included allowing counties to conduct primaries by mail, if certain conditions are met, and dispensing with the necessity of counting and tabulating votes in uncontested primaries. The subcommittee also addressed canvassing board procedures and recommended the legislature consider the issue of online voter registration and overhauling the active/inactive statute.

The full recommendations of all of the subcommittees are contained in complete detail in the body of this report.

As chair of the Election Reform Commission, I would like to personally thank the other Commissioners for their diligence and the quality of their work. Some of the Commission members had to travel long distances and be away from their homes and work for long periods of time.

Respectfully Submitted,

Ken Gordon

Election Reform Commission

Members of the Commission

Senator Ken Gordon, Chair

Bill Hobbs, Deputy Secretary of State, Vice-Chair

Bob Balink, El Paso County Clerk

Mark Baisley, President/CEO, Slipglass

Scott Doyle, Larimer County Clerk

Scott Gessler, Attorney, Hackstaff Gessler

Paul Hultin, Attorney, Wheeler, Trigg, Kennedy

Scott Martinez, Attorney, Holland and Hart

Sally Misare, Castle Rock Town Clerk

Patti Nickell, Bent County Clerk

Stephanie O'Malley, Denver County Clerk

Legislative Council Staff

Bo Pogue, Research Associate

Kurt Morrison, Senior Legislative Assistant

Table of Contents

	Page
Letter from the Chair.	v
Executive Summary.	1
Commission Overview and Charge.	2
Commission Activities.	3
Commission Recommendations.	4
Registration and Database.	4
Technology and Auditing.	5
Uniformity and Simplification.	7
Recommendations not Approved by Commission.	11
Technical Feasibility.	13
Fiscal Impact Statement.	15
Resources and Appendices.	16

This report is also available on line at:

http://www.state.co.us/gov_dir/leg_dir/lcsstaff/2009/comsched/09Electionsched.html



Senator Ken Gordon, *Chairman*
Bill Hobbs, Deputy Secretary of State, *Vice-Chair*
Bob Balink, El Paso County Clerk
Mark Baisley, President/CEO, Slipglass Enterprise
Information Security Architects
Scott Doyle, Larimer County Clerk

Scott Gessler, Attorney, Hackstaff, Gessler, LLC
Paul Hultin, Attorney, Wheeler, Trigg, Kennedy, LLP
Scott Martinez, Attorney, Holland and Hart, LLP
Sally Misare, Castle Rock Town Clerk
Patti Nickell, Bent County Clerk
Stephanie O'Malley, Denver County Clerk

Election Reform Commission

February 27, 2009

To the Members of the House and Senate State, Veterans, and Military Affairs committees:

Submitted herewith is the final report of the Election Reform Commission. This commission was created pursuant to Senate Bill 08-243 and is required to present its final report to the State, Veterans, and Military Affairs committees of the House and Senate no later than March 1, 2009. The Election Reform Commission is charged with reviewing, researching, and making recommendations to ensure that every eligible citizen has the opportunity to register to vote, participate in fair, accessible, and impartial elections, and have the assurance that his or her vote will count.

Respectfully Submitted,

Ken Gordon
Chair

Executive Summary

Commission Overview and Charge

The 11-member Election Reform Commission was created by Senate Bill 08-243 with a mission to "review, research, and make recommendations to ensure that every eligible citizen has the opportunity to register to vote, participate in fair, accessible, and impartial elections, and have the assurance that his or her vote will count." In fulfilling its mission, state law requires the commission to:

- conduct a nonpartisan review of the manner in which state and local elections are currently conducted;
- review research, data, and reports available on elections that may assist the commission in recommending changes to the state's election laws; and
- recommend changes to the state's election laws to protect the fundamental right to vote guaranteed by the state constitution by ensuring that every election conducted in the state is accurate, secure, transparent, verifiable, recountable, auditable, and accessible.

Senate Bill 08-243 contains a list of subjects that the commission may consider in conducting its review in the areas of voting technology, integrity, and alternatives and management.

Commission Activities

The Election Reform Commission met during the months of November 2008 through February, 2009, taking public testimony, hearing presentations from experts and stakeholder representatives in the fields of elections and voting technology, and deliberating on issues related to Colorado's elections system. The commission created three subcommittees, comprised of three commissioners each to address issues pertaining to:

- registration and database;
- technology and auditing; and
- uniformity and simplification.

Each of the subcommittees referred to the full commission a set of recommended changes to state election laws and practices in its assigned subject area. The commission then considered each subcommittee recommendation, taking action on which changes to state election law or practice it would recommend in the final report.

Commission Recommendations

The commission approved 20 recommendations, including 6 recommendations pertaining to registration and database, 2 recommendations pertaining to technology and auditing, and 12 recommendations pertaining to uniformity and simplification. The commission elected not to approve five recommendations.



Commission Overview and Charge

The 11-member Election Reform Commission was created by Senate Bill 08-243 (Appendix A). The bill establishes which authorities appoint the commission's membership and the criteria to be considered in appointing members. The mission of the commission is to "review, research, and make recommendations to ensure that every eligible citizen has the opportunity to register to vote, participate in fair, accessible, and impartial elections, and have the assurance that his or her vote will count." In fulfilling its mission, state law requires the commission to:

- conduct a nonpartisan review of the manner in which state and local elections are currently conducted;
- review research, data, and reports available on elections that may assist the commission in recommending changes to the state's election laws; and
- recommend changes to the state's election laws to protect the fundamental right to vote guaranteed by the state constitution by ensuring that every election conducted in the state is accurate, secure, transparent, verifiable, recountable, auditable, and accessible.

State law contains the following list of subjects that the commission may address in conducting its required review:

Voting technology.

- issues and problems involving electronic voting systems that have arisen in Colorado and other states since the enactment of the federal Help America Vote Act of 2002 (HAVA);
- the standards, criteria, and procedures by which rules and guidelines for the certification of electronic voting systems are adopted in the state;
- the manner in which electronic voting systems are certified in Colorado;
- public access to the certification process and to electronic voting system software;
- technology that enables persons with disabilities to vote independently and in compliance with HAVA; and
- the short- and long-term costs of purchasing, maintaining, and operating electronic voting systems.

Integrity.

- the reliability and integrity of electronic and other voting systems;
- the security, accuracy, and efficiency of the systems and methods used to register electors and to maintain voter registration records;
- whether the auditing and recounting procedures in current law provide a meaningful level of statistical confidence to electors and candidates;
- the number of eligible electors who show a form of identification that does not contain a photograph of the eligible elector when voting at a polling place, and the number of eligible electors who show each form of such identification, based on information received from county clerk and recorders; and
- other issues related to the accuracy, security, transparency, verifiability, recountability, auditability, and accessibility of elections in the state.



Alternatives and management.

- issues related to the conduct of elections in special districts;
- whether the state should adopt a uniform voting system to be used in all counties;
- alternative methods of conducting elections; and
- the feasibility and desirability of creating a permanent election reform commission.

Senate Bill 08-243 requires presentation of this final report to the State, Veterans, and Military Affairs committees of the Senate and House of Representatives.

Commission Activities

The commission met six times during the months of November 2008 through February 2009. The commission took public testimony at four of these meetings, and specifically fielded testimony from county clerk and recorders in conjunction with the Colorado County Clerks Association annual conference in January, 2009. The commission also heard presentations from several experts and representatives of stakeholder organizations in the fields of elections and election technology. A compilation of the commission's meeting activities can be found in the Resources and Appendices section of this report.

At the commission's November 12, 2008, meeting, the commission created three subcommittees, comprised of three commissioners each to address issues pertaining to:

- registration and database;
- technology and auditing; and
- uniformity and simplification.

The subcommittees were charged with establishing a set of recommended changes to state election laws and practices in their assigned subject areas for referral to the full commission. The commission took action on the referred recommendations at its February 17, 2009, meeting. To take final action on the subcommittee recommendations, the commission created a ballot consisting of action items representing all of the recommendations made by the three subcommittees. The commission approved 20 of the recommendations, and elected not to approve 5 of the recommendations. Several of the recommendations approved by the commission do not recommend direct legislative action by the General Assembly, but rather recommend that the General Assembly consider certain issues.



Commission Recommendations

As a result of the Election Reform Commission's activities, the commission makes the following recommendations to the Colorado General Assembly, organized by subcommittee subject area. The full subcommittee recommendations, as submitted to the full commission, are contained in Appendix B (Registration and Database), Appendix C (Technology and Auditing), and Appendix D (Uniformity and Simplification).

Registration and Database

Recommendation #1 – SCORE System

The Statewide Colorado Registration and Elections (SCORE) system was implemented in 2008 to comply with the federal Help America Vote Act of 2002 (HAVA). SCORE is a database containing statewide voter registration information, which is used for identity verification.

The commission encourages and supports the efforts of the Secretary of State and the county clerk and recorders to continue making improvements to the system in the following areas:

- improvement of reporting capabilities;
- refinement and development of additional modules; and
- resolution of technical issues.

Recommendation #2 – Photo Identification

The commission recommends legislation to require voters to present photo identification when registering to vote.

Recommendation #3 – Voter Registration Form

Prior to the 2008 general election, confusion existed regarding the need for new voters to check a box on voter registration forms affirming that they did not have a Colorado driver's license or Department of Revenue identification number if they were submitting the last four digits of their social security numbers in lieu of these forms of identification.

The commission recommends that the Secretary of State and the Colorado County Clerks Association work to redesign the Colorado voter registration form to:

- clarify issues surrounding the affirmative need to mark the "check box" if a voter does not have a driver's license or state identification number. The commission also recommends that voter instructions be rewritten to clarify that a driver's license or state identification number is required if one has been issued, and a social security number should only be used if the voter has not been issued the required documents; and
- use a separate form to make administrative changes to information for currently registered voters, including changing a name, address, or party affiliation.



Recommendation #4 – Assisted Living Facilities

The commission recommends that the General Assembly consider legislation to exempt persons living in assisted living or nursing care facilities from identification requirements for voting. In addition, the commission recommends the use of the Secretary of State's rules to ensure consistent application of regulations pertaining to identifying residents of assisted living or nursing care facilities for elections-related purposes.

Recommendation #5 – Verification Period for UOCAVA and ID-deficient Voters

The commission recommends legislation to expand the current eight-day post-election signature verification period to allow for continued receipt of ballots from overseas voters under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), while maintaining the requirement that the ballots be postmarked no later than 7 p.m. on election day, where postmarks are applicable. The commission also recommends providing identification to voters who are identification-deficient.

Recommendation #6 – National Voter Registration Database

A national voter registration database would eliminate the possibility of citizens registering to vote in more than one jurisdiction.

The commission recommends that Colorado participate in the implementation of a national voter registration database.

Technology and Auditing

Recommendation #7 – Voting system certification

After the Secretary of State's December 2007 decertification of the electronic voting systems (EVS) used by the majority of Colorado counties, Governor Ritter signed into law House Bill 08-1155, which provided for retesting and interim re-certification of any decertified voting machines. Under current law, the provisions of the bill are repealed on July 1, 2009, resulting in the decertification of systems certified under the bill. Extending the interim emergency certifications allowed for in HB 08-1155 will provide financial relief to cash-strapped counties and ample time to phase in the next generation of technology.

The commission recommends legislation to amend the statutes on voting system certification as follows:

- **House Bill 08-1155.** Extend the interim emergency certifications provided for in House Bill 08-1155 through the 2013 election cycle. Under this recommendation, use of currently certified EVS would be allowed through the 2013 election cycle, subject to all conditions that attached to the 2007 and 2008 certifications of such EVS.
- **Voter-verified paper audit trails (VVPATs).** Repeal the requirement that all direct recording electronic (DRE) voting equipment have voter-verified audit trails (VVPATs) by 2010. Jefferson and Arapahoe counties will not have to perform expensive short-term retrofits on DREs not currently equipped with VVPATs.



- ***Paper ballot/optical scan-based EVS.*** For all elections after the 2013 election cycle, and for all new electronic voting systems purchased and utilized before the 2013 election cycle, require all counties to utilize a paper ballot/optical scan-based electronic voting system that has been certified under the revised procedures recommended below.
- ***Certification of paper ballot/optical scan-based system and modification of EVS whose certifications have been extended.*** (applies to all new EVS and modifications to certified EVS)
 - ▶ repeal requirement that all EVS must be tested and certified as meeting current federal standards;
 - ▶ allow EVS whose certifications are extended through the 2013 election cycle to be modified subject to testing and certification by the Secretary of State that the systems, as modified, meet all Colorado testing and certification requirements;
 - ▶ change the testing and certification completion requirement in Section 1-5-617 (1)(c), C.R.S., from 90 days to 180 days; and
 - ▶ allow the Secretary of State to utilize and rely upon testing done by another state's secretary of state or chief election official, or by a federally certified testing lab, provided that the Colorado Secretary of State has complete access to all test documentation, test data, and test reports, and provided that the Colorado Secretary of State makes written findings and certifies that (1) he or she has reviewed the test documentation, data, and reports and finds that the testing has been conducted in accordance with state-of-the-art engineering standards and practices; and (2) the testing met each applicable Colorado requirement.

Recommendation #8 – Post-election audits

The commission recommends legislation to revise the statutory requirements for post-election audits in Section 1-7-514, C.R.S., to require a risk-based audit methodology instead of the current fixed-percent audit. All aspects of each election, whether mail-in voting, early voting, election day voting, or other, should be subject to the same audit requirements. In addition, the commission recommends the following:

- require all voting systems to report votes in auditable batches;
- define the confidence level required, e.g. 90 percent or some lesser confidence level;
- require audit units to be randomly selected;
- require the audit process to be transparent;
- require audit processes to be developed for each voting system in Colorado and accomplished in a way that is easily understood by public officials charged with completing the work;
- set out in statute the general requirements, standards, and procedures for a risk-based audit; and



- require the Secretary of State to implement risk-based election audits by notice and comment rule-making, resulting in a new election rule giving guidance to the counties as to the specific requirements, standards, and procedures to be followed.

Uniformity and Simplification

The Election Reform Commission feels that certain areas within the elections environment are primed for uniform and consistent practices. While the commission recognizes the need for designated election officials to have flexibility in deciding how best to deliver elections in their respective counties, a need exists to have consistent practices where there is an opportunity to curtail voter confusion.

Recommendation #9 – Mail Ballot Elections

The commission recommends legislation to allow counties the option to conduct primary elections by mail, if the legislation contains the following requirements:

- ***Minimum threshold.*** Before an all-mail ballot election is allowed, the absentee voter participation in the county must exceed 50 percent of all active voters in the previous presidential or gubernatorial election.
- ***Service centers.*** Counties conducting elections by mail must include a sufficient number of service centers established by formula. The service centers must provide consistent services to the voting public, and each service center must have secured computer access, be Americans with Disabilities Act-compliant, include a sufficient number of DREs, include a sufficient number of voting booths, have the ability to distribute second original ballots, have the ability to distribute replacement ballots, serve as a ballot drop-off location, and provide the ability to register in an emergency manner. In addition, the legislation must:
 - require minimum hours of operation and number of days open prior to election day;
 - require service centers to be available during early voting; and
 - require designated election officials to determine the number, location, and manner of operation of service centers, including poll watching activities at service centers, in consultation with the chairpersons of the county central committees of the major political parties and representatives of the minor political parties, and after a public comment period of no less than 15 days and a public hearing held in accordance with the rules adopted by the Secretary of State.
- ***Election preparation.*** Designated election officials must meet with an election vendor to determine whether the vendor has the ability to provide sufficient mail ballots in a timely manner, and meet with the U.S. Postal Service to coordinate ballot mailing, receiving, and tracking.
- ***Voter eligibility.*** The legislation must include language specifically mandating who is to receive mail ballots. The language must include direction to the designated election official that he or she mail to all registered voters, mail to all active voters, or that the



county maintains discretion as to whether to provide a mail ballot to active or inactive eligible voters or active *and* inactive eligible voters. The legislation should also retool the manner by which Colorado currently approaches its "active/inactive" voter registration designations. New legislation should take into account the existence of SCORE, its functionality, and its ability to aid in list maintenance and national change of address tracking.

- **Unaffiliated voters.** The legislation must establish deadlines for affiliating with a party when conducting a mail ballot election.
- **Issuing/counting ballots.** The legislation should allow designated election officials to send ballots as early as 30 days prior to the election, and bulk mailing no later than 21 days prior. The legislation should address how a voter requests a replacement ballot (i.e., by telephone, internet, or facsimile), and allow designated election officials to begin counting ballots as soon as received or at least 22 days before the election.
- **Return of ballots.** The legislation should require uniformity related to methods of returning ballots. At a minimum, each polling location/service center must have a secure receptacle for voters to cast or drop off their mail ballots, and the security of the receptacle must be consistent with the security of paper or provisional ballots under current law or Secretary of State rule. Also, the legislation should consider stand-alone return boxes and the possibility of creating a certification program for ballot collection drives.
- **Postage.** The legislation should require (or allow) counties to pay postage, with the state reimbursing counties if it is a requirement.
- **Homeless voters.** The legislation should address services for homeless voters, including allowing such voters to list the county clerk's office as the mailing residence for obtaining a mail ballot.

Recommendation #10 – Healthcare Facilities

Colorado's counties define the term "health care facilities" differently across the state, resulting in a variance in the treatment of eligible voters in these venues. The commission recommends that the term "health care facilities" be specifically defined in statute.

Recommendation #11 – Forms

Forms used prior to and during the 2008 election cycle were very confusing to voters and in some instances caused voter disenfranchisement. Several forms, including voter registration forms, applications for mail ballots, combination forms, provisional ballot forms, and provisional ballot envelopes, varied across the state.

The commission recommends legislation to address election forms, including voter registration, mail ballot application, combination, and provision ballot forms, with the following provisions:

- The Secretary of State must dedicate resources to obtaining professional guidance for the development of forms that minimize voter confusion and maximize ease of use.



The legislation must also require the Secretary of State to obtain professional guidance in developing the forms.

- The legislation must require rule making regarding what constitutes approved and acceptable forms certified for use and acceptance by eligible voters, campaigns, voter registration drives, and designated election officials.
- The legislation must establish uniformity with regard to how forms are used inside polling locations, particularly the management of provisional ballot forms and envelopes by election judges and personnel.

Recommendation #12 – Primary Elections

Currently, county clerk and recorders must hold primary elections, even if there is no contested race in the primary. The commission considered the following three methods for allowing a county clerk and recorder to designate the winner of an uncontested primary election without conducting an election:

- cancelling the primary election;
- holding the primary election in the legal sense, but allowing the clerk and recorder to dispense with collecting or tabulating votes; or
- holding the primary election, but limiting all votes to a single polling location, thus creating a single polling center.

The commission selected the second option for recommendation to the General Assembly. This approach avoids major statutory changes and the unintended consequences of actually cancelling a primary, while eliminating any incentive for a candidate or party to manipulate a primary for campaign finance purposes.

Therefore, the commission recommends that a clerk and recorder be allowed to designate the winner of an uncontested primary election by holding a primary in a legal sense, but allowing the clerk and recorder to dispense with collecting or tabulating votes.

Issue #13 – Canvassing Board Procedures

Canvass board procedures for partisan elections are poorly defined. The commission recommends legislation to address the need for uniformity and simplicity with regard to canvass board procedures. The legislation should include the following provisions:

- ***Composition of canvass board.*** The legislation must explicitly require clerk and recorders to tell county chairs the number of canvass board members necessary to complete work, and require the county chairs to each appoint the same number of members. Currently, the major party chairpersons are required to appoint one or more members and certify their appointment "in the manner prescribed by the clerk and recorder." Current law allows each party chairperson to appoint as many as six canvass board members as he or she sees fit. In practice the number of appointees and procedures vary considerably, and in some instances there are too few canvass board members to meaningfully complete the work in the allotted time.



- **Decision-making procedures.** The legislation should specify proper procedure for reaching decisions and provide for uniform application of how members are counted. The law is silent on how the canvass board reaches decisions. Currently, the board consists of members appointed by the chair, plus the clerk and recorder. Thus, if the canvass board operates by majority vote, the clerk and recorder can easily and consistently be outvoted. In some instances, canvass boards treat all Republicans as one vote, all Democrats as one vote, and the clerk and recorder as one vote. In other instances, certification may require unanimity.
- **Duties of canvass board.** In addition to the current canvass board duties of reconciling the ballots to confirm that the number counted does not exceed the number cast and certifying the abstract of votes, the legislation should stipulate one of the following:
 - require the boards to ensure the number of ballots cast in each precinct does not exceed the number of eligible voters in any precinct; or
 - allow canvass boards to inspect and investigate where the number of votes cast fails to align with the number of eligible voters.
- **Remedies for improper certification.** The legislation should allow minor party and unaffiliated candidates to bring objections to the canvass board process to the Secretary of State, who will then investigate and resolve any procedural problems. Under current law, minor party and unaffiliated candidates may appoint observers to the canvass board process, but the law is silent if they have an objection. Assumably, a minor party candidate may bring a district court complaint under Section 1-1-113, C.R.S., or a person may wait until certification and contest the election results. Allowing an intermediate, regulatory remedy rather than requiring a full-blown district court hearing or election contest is appropriate.
- **Remedies for failure to certify.** The legislation should explicitly require the canvass board to either certify election returns or transmit to the Secretary of State noncertified results with an explanation for the noncertification. The law is silent if a canvass board refuses to certify the returns. Under Section 1-10-104, C.R.S., the law directs that if the results do not conform to law, the canvassing board will still canvass the returns if they are explicit enough in showing the number of votes cast. But this section nonetheless leaves unanswered whether a canvass board must certify defective returns, or what the Secretary of State's remedies are if the canvass board refuses to certify.

Recommendation #14 – Online voter registration

The commission recommends that the General Assembly take into consideration the issue of allowing on-line voter registration.

Recommendation #15 – Future SCORE funding

The commission recommends that the General Assembly consider providing a source of funding to maintain the SCORE system after the existing funding source is exhausted. The General Assembly should also consider whether counties should uniformly be required to contribute funding to support SCORE.



Recommendation #16 – Overhaul Active/Inactive Statute

The commission recommends that the General Assembly consider a major re-haul of Colorado's active/inactive statute.

Recommendation #17 – Overhaul Title 1, C.R.S., in its Entirety

The commission recommends that the General Assembly consider the issue of requiring the Secretary of State to form an ongoing working group to engage in serious work to re-haul Title 1, C.R.S., and that the Secretary of State, along with the legislature, continue to advocate for significant revisions guided toward bringing uniformity and simplicity to the elections environment in the state.

Recommendation #18 – Tribal Identification

The commission recommends that the General Assembly consider the issue of expanding the acceptable form of identification required for voter registration to include tribal identification cards issued by a federally recognized Indian tribe that certifies that the eligible elector is a member of the tribe and is at least 18 years of age at the time of the election.

Recommendation #19 – Uniform Notice and Correction of Deficiencies

The commission recommends that the General Assembly consider the issue of creating uniformity across all counties with regard to the following:

- which deficiencies in voter registration information can be cured and which deficiencies are fatal to registration;
- the manner in which voters are informed that identification is required to be included in mail ballots; and
- what types of locations are suitable for dropping off mail ballots on election day.

Recommendation #20 – Extension of commission

One of the subjects suggested for review by the Election Reform Commission in Senate Bill 08-243 is "the feasibility and desirability of creating a permanent Election Reform Commission." The commission is currently set to expire on July 1, 2009.

The commission recommends the creation of a permanent Election Reform Commission.

Recommendations Not Approved by the Commission

Five additional recommendations were presented to the Election Reform Commission for consideration at its February 17, 2009, meeting. However, the commission elected not to approve these recommendations.



Exhibit 5



Suggestions for Better Election Security

From the Vulnerability Assessment Team at Argonne National Laboratory

Summary of Common Security Mistakes

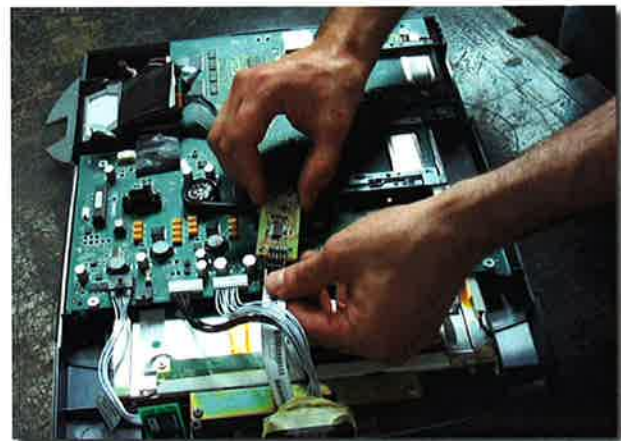
1. Electronic voting machines that fundamentally lack security thought and features, including an ability to detect tampering or intrusion, or to be reliably locked or sealed.
2. Failure to disassemble, examine, and thoroughly inspect (not just test) a sufficient number of voting machines before and after elections in order to detect hardware or software tampering.
3. Assuming that tamper-indicating seals will either be blatantly ripped/smashed open, or else there is no tampering. In reality, even amateurs can spoof most seals leaving (at most) subtle evidence.
4. Inadequate seal use protocols and training of seal installers and inspectors. Failure to show examples of blatantly and subtly attacked seals to seal inspectors.
5. Over confidence in use of a voter verified paper record (VVPR). A VVPR is an excellent security countermeasure, but it is not a silver bullet, especially for an election organization with poor overall security.
5. Little or no insider threat mitigation.
6. A poor security culture, including denial and no *a priori* procedures for dealing with security questions or concerns.

About These Suggestions

The following suggestions for better election security are from the Vulnerability Assessment Team (VAT) at Argonne National Laboratory (<http://www.ne.anl.gov/capabilities/vat>). The suggestions fall into two categories, "Minimum", which are security features that are essential in our view, and "Recommended", which are needed for the best security.

Hardware & Software Inspection

Recommended: Prior to the election, at least 1% of the voting machines—randomly chosen—should be removed from the



Inserting alien electronics into an electronic voting machine in a classic (non-cyber) "man-in-the-middle" attack.

polling places and tested, then disassembled, inspected, and the hardware examined for tampering and alien electronics. The software/firmware should also be examined, including for malware. It is not sufficient to merely test the machines in a mock election, or to focus only on cyber security issues! This analysis should be completed prior to the election.

Minimum: It is completed less than 6 weeks after the election.

Minimum: Within 4 weeks after the election, at least 1% of the voting machines actually used in the election—randomly chosen—should be tested, then disassembled, inspected, and the hardware examined for tampering and alien electronics. The software/firmware should also be examined, including for malware. It is not sufficient to merely test the machines in a mock election, or to focus only on cyber security issues!

Recommended: The voting machines for the above inspection (or trial bribery discussed below) should be randomly chosen based on pseudo-random numbers generated by computer, or by hardware means such as pulling numbers or names from a hat. No individual should

make the random choices without the aid of hardware or software.

Insider Threat

Minimum: All election officials, technicians, contractors, or volunteers who prepare, maintain, repair, test, inspect, or transport voting machines, or compile “substantial” amounts of election results should have background checks, repeated every 3-5 years, that include a criminal background history, credit check, and (when practical) interviews with co-workers.

Minimum: Prior to each election, all poll workers, election judges, election officials, and relevant contractors and technicians should take an oath to protect election integrity. They should be warned of the legal penalties for vote tampering and fraud, and reminded of their patriotic and ethical responsibility to help guarantee fair elections. They should also be thanked for taking on this important responsibility, and being vigilant of election security.

Minimum: Before each election, the U.S. citizenship of every poll worker and election judge should be verified in a reliable manner.

Recommended: On a regular basis, try bribing a small subset of poll workers, election judges, election officials, technicians, clerks, and personnel who transport voting machines and other election materials. Let them keep the money and hail them publicly as honest heroes if they decline the bribe. (Allow at least 36 hours for the bribe to be reported or declined.) There are legal entrapment issues here, but the point isn't so much to identify and fire dishonest individuals as it is to make bribes untenable by creating publicity and uncertainty about whether an apparent bribe is some kind of test.

Recommended: A written policy should be in effect and periodically communicated to all employees and contractors that bribery attempts must be reported immediately, and where or to whom they should be reported.

Locks

Minimum: Locks on voting machines should not all open with the same key.

Minimum: Opening of a lock on a voting machine or container should be accompanied by a careful examination of the exterior of the voting machine or container in order to try to determine if the integrity of the voting machine or container has been compromised without disturbing the lock. This includes looking for evidence of cosmetic repair of the

voting machine or container walls after they have been breached. Election officials, judges, and technicians should be trained on how to inspect the relevant voting machines or containers, including the underside.

Tamper-Indicating Seals

For information on tamper-indicating seals, see *American Scientist* **94**(6), 515-523 (2005); *ACM Transactions on Information and System Security*, **14**, 1–29 (2011); <http://www.cs.princeton.edu/~appel/voting/Johnston-AnalysisOfNJSeals.pdf> and <http://www.ne.anl.gov/capabilities/vat>.

Minimum: Avoid the assumption that tamper-indicating seals will either be blatantly ripped/smashed open, or else there is no tampering. In reality, even amateurs can spoof most seals leaving (at most) subtle evidence.

Minimum: Prior to each election, all poll workers and election officials who inspect seals (including tamper-evident packaging) need to have a minimum of 10 minutes of training per kind of seal used. This training will include information as to how to install (if appropriate) and inspect the seal. This should include multiple samples, photos, or videos of that specific kind of seal that has been attacked subtly and samples, photos, or videos of that specific kind of seal that has been attacked blatantly, e.g., by being ripped open or smashed.

Minimum: Personnel who inspect seals that protect “large” numbers of election results should have an additional 10 minutes per kind of seal. This should include hands-on practice in spotting sample seals that have been opened subtly and those that have been opened blatantly.

Recommended: Only a small number of election officials should be authorized to order tamper-indicating seals, and the seal manufacturer or vendor should contractually agree to refuse orders not placed by those individuals or by anyone who does not know the secret password required for seal purchases for a given election district, and to report failed attempts to officials of that election district.

Recommended: The vendor or manufacturer of seals used for election purposes should contractually agree not to provide 2 or more seals with the same serial number (including at a later time) to anyone.

Recommended: A two-person rule should be in effect when a seal is applied to critical election assets. Each person should verify that the correct seal was correctly applied, and that its

serial number is correctly entered into the database of seal serial numbers.

Minimum: Only tamper-indicating seals with unique serial numbers should be used.

Recommended: Signing or initialing seals offers little effective security and should not be done.

Minimum: All seal inspections require checking the seal serial number against the secured data log of seal serial numbers. Each seal must also be carefully examined for evidence of both subtle and blatantly obvious opening, counterfeiting, damage, or removal.

Minimum: The list of seal serial numbers for seals applied to voting machines and containers or packages of sensitive election materials must be carefully protected from tampering, theft, or substitution.

Recommended: Seals should not be used in sequential order based on serial number (so that an adversary cannot predict a seal serial number in advance).

Minimum: Seal inspectors must not be fooled by a seal of the wrong kind or color that has the correct serial number—a common mistake.

Minimum: Seals must be inspected alongside an identical (except for serial number), well-protected unused seal of the same kind. There must be a comparison of size, morphology, color, surface finish, and serial number font, digit spacing, and digit alignment/orientation.

Recommended: Minimize the use of (pressure sensitive) adhesive label seals (because these tend to be easy to counterfeit or to remove, then replace without leaving easily detectable evidence, plus they require an inordinate amount of training and inspection time to be effective).

Minimum: With adhesive label seals, prior to installing the seal, the surface the seal is to be applied to must be cleaned and checked for evidence of oil or other substances that can reduce surface adhesion.

Minimum: With adhesive label seals, the way the seal behaves when it is removed is often a critical method for checking for tampering. To be effective, however, the seal inspector must know how the seal is supposed to behave when removed.

Minimum: Any checking of a seal for evidence of being broken or tampered should be accompanied by a careful examination of the container or package or voting machine the seal is attached to in order to try to determine if the integrity of the container or package or voting machine has been compromised without disturbing the seal. This includes looking for evidence of cosmetic repair of the container/package/voting machine walls after they have been breached. Seal inspectors should be trained on how to do this inspection for each kind of container, package, or voting machine.

Minimum: All used seals should be preserved until at least 3 months after the election for possible examination, then thoroughly destroyed (not just discarded in the trash) so that the parts cannot be used by adversaries to practice or execute seal attacks.

Minimum: All unused seals should be protected or guarded prior to use from theft or unauthorized access. Seal installers must be required to protect and turn in any unused seals.

Secure Transport

Recommended: Escort the voting machines to and from the polling place if at all possible. Use *pro bono* volunteers if necessary.

Recommended: Do not allow technicians to work on a specific voting machine without authorization and oversight.

Recommended: Personnel or contractors who transport voting machines to or from the polling places should be bonded.

Minimum: Some individual or group should be responsible for accepting voting machines and sensitive election materials delivered to the polling place before or on election day, sign for them, and be responsible for providing oversight to the extent practical. (This can include students at a school, for example.) It should be possible to determine if there was an unexpected delay in delivery of any such voting machines or election materials, and this delay must be investigated immediately. Similarly, any delay in receipt of the voting machines back at the storage warehouse after the election should be detectable and immediately investigated.

Chain of Custody

A chain of custody is a process that helps to secure voting machines, ballots, records, memory devices, seals, keys, seal databases with serial numbers, and other election materials. We henceforth refer to these items needing protection from theft, tampering, copying, or substitutions as “assets”. (Note:

A “chain of custody” is not a piece of paper that multiple people sign or initial.)

Recommended: An effective chain of custody starts by checking that everyone to be involved in handling the assets in question is trustworthy. This is best determined by periodic background checks.

Minimum: An effective chain of custody requires procedures to make sure that each person handing off the assets to another is sure of the identify of the person they are handing the material to, and that this person has been authorized to receive the assets.

Recommended: Each individual in the chain of custody must know the secret password of the day or the election before being allowed to take control of the assets.

Minimum: Each individual in the chain of custody must assume the individual responsibility of safeguarding the assets while in their custody, not letting the assets out of their sight to the extent possible, and securing the assets under lock or seal when not in sight.

Minimum except where noted: A chain of custody log should be kept with the assets. It must be signed by each recipient in the chain of custody when accepting the assets with a carefully signed signature (not initials) along with a printed, legible listing of their name, the date, location (Recommended), and time (Recommended). This log must also be protected from tampering, counterfeiting, or substitution.

Independent Security Review

Minimum: The majority of advice on election security should not come from vendors or manufacturers of voting machines or of tamper-indicating seals or other security products used in elections. It is necessary to seek out objective, independent security expertise and advice.

Minimum: Election officials will arrange for a local committee (*pro bono* if necessary) to serve as the Election Security Board. The Board should be made up primarily of security professionals, security experts, university professors, students, and registered voters not employees of the election process. The Board should meet regularly to analyze election security, observe elections, and make suggestions for improved election security and the storage and transport of voting machines and ballots. The Board needs considerable autonomy, being able to call press conferences or otherwise publicly discuss its findings and suggestions as appropriate.

Employees of companies that sell or manufacture seals, other security products often used in elections, or voting machines are not eligible to serve on the Board.

Minimum: At least once every 3 years, the Election Security Board should oversee or conduct a comprehensive vulnerability assessment of the local election process, involving external consultants, volunteers, and security experts (including *pro bono*) to the extent practical.

Minimum: A Chief Election Security Officer (paid or unpaid) should be appointed who may have other duties as well. He or she is responsible for analyzing and overseeing election security issues and security training. The Security Officer also deals with and investigates security questions, concerns, and incidents on election day. He/she serves on the Election Security Board (discussed above) as a voting member, but does not chair the Board or appoint its members.

Recommended: The Chief Election Security Officer should maintain a publicly posted, frequently updated list of what he/she judges as the ten best suggestions (from the Board, or other internal or external sources) for potentially improving election security, and the prospects for implementing them. Public comments on this list should be encouraged.

Creating & Nurturing an Effective Security Culture

The key to good security is to have a healthy security culture. This requires everyone to pay attention to security issues, be thinking critically and continuously about security, to ask good questions, avoid denial, and to be free to raise concerns and be listened to about security issues.

Minimum: When election security is questioned, the first response of election officials and the Chief Election Security Officer must not be to deny the possibility of security vulnerabilities, but rather to seek to learn more and solicit advice from the person(s) raising these questions (and others) as to possible countermeasures or security improvements.

Recommended: Before each election, discuss in some detail with poll workers, election judges, and election officials the numerous ways that the voting process can be tampered with, and what to watch out for. Have them individually, or in groups suggest other ways they would tamper with votes if they were so inclined, including fanciful ways, using insiders or outsiders or insiders collaborating with outsiders. (The merits of the attack scenarios they devise are less important than instilling a mindset of thinking like the bad guys).

Recommended: Poll workers, election judges, election officials, and other personnel involved in running elections should be warned and educated about techniques for misdirection and sleight-of-hand, perhaps by having these techniques explained/demonstrated by a magician, live or on video. (The sense of alertness to malicious acts that this engenders is actually of greater benefit than awareness of misdirection and sleight-of-hand *per se*, though the latter is not negligible.)

Recommended: Before each election, discuss with poll workers, election judges, and election officials the importance of ballot secrecy, and the importance of watching for miniature wireless video cameras in the polling place, especially mounted to the ceiling or high up on walls to observe voters' choices. The polling place should be checked for surreptitious digital or video cameras at least once on election day.

Recommended: Poll workers, election judges, election officials, and other personnel involved in running elections should be told how to accurately verify the identity of authorized election and law enforcement officials, as well as election workers who may be present on election day.

Recommended: Security must not be based substantially on secrecy, i.e., Security by Obscurity is not a viable security strategy, nor is secrecy conducive to observers, critical review, process improvement, feedback, transparency, or accountability. Somewhat counter-intuitively, the best security is security that is transparent. (Note: Some short-term secrecy may be warranted, such as short-term passwords or secrecy about the details of voting machine transport.)

Minimum: Security is hard work so expect it to be hard work. Any security device, system, procedure, or strategy that sounds too good to be true almost certainly is.

Minimum: There must be a convenient way for poll workers, election judges, election workers and contractors, election officials, and the general public to report security concerns, including anonymously on election day. There must be mechanisms in place to respond in a timely manner to these concerns, perhaps through the Chief Election Security Officer discussed above.

Recommended: Welcome, acknowledge, recognize, praise, and reward good security practice, as well as reasonable security questions and suggestions from any quarter, including from employees, contractors, poll workers, election judges, journalists, bloggers, and the general public.

Recommended: Election officials are often elected or are political appointees. It is important for a good security culture to attempt to differentiate and separate concerns, questions, and criticisms about election security from political attacks on those election officials.

Recommended: Security is difficult and involves complicated, value-based tradeoffs. Thus, security policy and practice is intrinsically a controversial topic worthy of debate and analysis, and should be viewed and treated as such. The existence of disagreement and dissent in regards to security must not be taken as a sign of weakness, but rather welcomed as a sign of a healthy security culture.

Other Suggestions

Recommended: Election officials should pressure manufacturers of voting machines to design them with better physical security, cyber security, and tamper/intrusion detection. Insist that manufacturers of voting machines design them with secure hasps that allow the use of locks and seals other than pressure sensitive adhesive label seals.

Minimum: Poll workers, election judges, and election officials should be able and expected to determine if a voting machine has been replaced by an unauthorized voting machine or counterfeit voting machine.

Recommended: A hash should be printed on each paper ballot on election day after each voter has completed the ballot. This hash should be generated from a secret algorithm that is different for each election, and possibly each polling location.

About the Vulnerability Assessment Team

The Vulnerability Assessment Team (VAT) at Argonne National Laboratory has conducted vulnerability assessments on approximately 1000 different physical security and nuclear safeguards devices, systems, and programs. This includes analyzing locks, anti-counterfeiting tags, tamper-indicating seals, RFIDs, GPS, microprocessor systems, contact memory buttons, electronic voting machines, nuclear safeguards equipment, and biometrics and other access control devices. The VAT has demonstrated how all these technologies can be easily defeated using widely available tools, materials, and supplies, but has also devised and demonstrated simple and practical countermeasures.

In addition, the VAT has provided security consulting, training, R&D, specialty field tools, and novel security devices and approaches for more than 50 different companies, NGOs, and

government organizations, including DoD, NNSA, DHS, U.S. Department of State, the International Atomic Energy Agency (IAEA), Euratom, and intelligence agencies.

VAT personnel have given over 80 invited talks (including 6 Keynote Addresses) at national and international conferences.

The VAT is frequently interviewed by journalists and security bloggers about its work and its views on security. See, for example:

“Diebold Voting Machines Can Be Hacked by Remote Control”,
http://www.salon.com/news/2012_elections/index.html?story=/politics/elections/2011/09/27/votinghack

Bradblog.com, <http://www.bradblog.com/?p=8785>,
<http://www.bradblog.com/?p=8790>,
<http://www.bradblog.com/?p=8818>

“Most Security Measures Easy to Breach”,
<http://www.youtube.com/watch?v=frBBGJqkz9E>

“Roger Johnston on Election Security”,
<http://www.opednews.com/articles/Argonne-Lab-s-Head-of-Vuln-by-Joan-Brunwasser-110329-968.html>

“Getting Paid to Break Into Things: How Vulnerability Assessors Work at Argonne National Lab”,
http://www.techrepublic.com/blog/security/getting-paid-to-break-into-things-how-vulnerability-assessors-work-at-argonne-national-lab/5072?tag=mantle_skin;content

“Closing the Curtains on ‘Security Theater’”,
<http://www.smartplanet.com/technology/blog/science-scope/at-argonne-national-lab-closing-the-curtains-on-security-theater/5167/>

“Digital Privacy: Are You Ever Alone?”,
<http://news.medill.northwestern.edu/chicago/news.aspx?id=187163>

“Six Rising Threats from CyberCriminals”,
http://www.computerworld.com/s/article/9216603/Six_rising_threats_from_cybercriminals

“Roger Johnston on Security Vulnerabilities of Electronic Voting”, <http://blog.verifiedvoting.org/2010/10/15/1131>

“Phishing Attacks: Training Tips To Keep Your Users Vigilant”,
<http://www.techrepublic.com/blog/security/phishing-attacks-training-tips-to-keep-your-users-vigilant/5402>

Roger Johnston interviewed live on WTTW Public Television’s “Chicago Tonight” program about electronic voting machines,

<http://www.wttw.com/main.taf?p=42,8,80&pid=BMeOsuVOgSubQammoGQxMIIX00avS55H>

“IT Security: Maxims for the Ages”,
<http://blogs.techrepublic.com.com/security/?p=2435>

“Security Maxims”, *Security Now!* Podcast #215,
<http://www.grc.com/sn/sn-215.htm>

“Vulnerability Assessment’s Big Picture”, *CSO Magazine*,
http://www.csoonline.com/read/060107/fea_qa.html



Argonne National Laboratory

About Argonne National Laboratory

Argonne National Laboratory, the nation’s first national laboratory, is one of the U.S. Department of Energy’s largest national laboratories for science and engineering research. It is located 25 miles from downtown Chicago. Argonne is managed by UChicago, LLC, for the United States Department of Energy.

Argonne has approximately 3,400 employees, including 1,100 scientists and engineers, three-quarters of whom hold doctoral degrees. Argonne’s annual operating budget exceeds \$738 million.

Since 1990, Argonne has worked with more than 700 companies, federal agencies, and other organizations.

