



DENVER
THE MILE HIGH CITY

John W. Hickenlooper
Mayor

CITY AND COUNTY OF DENVER

CLERK and RECORDER ELECTIONS DIVISION

Stephanie Y. O'Malley
CLERK and RECORDER

303 W. Colfax Ave, Dept 101
Denver, Co. 80204

TELEPHONE: 720-913-8683
FAX: 720-913-8600

January 16, 2008

The Honorable Mike Coffman
Secretary of State
Department of State
State of Colorado
1700 Broadway, Suite 250
Denver, CO 80290

Re: Request for Reconsideration of the December 17, 2007, Decision regarding the voting systems of Sequoia Voting Systems, Inc.

Dear Secretary Coffman:

Pursuant to C.R.S. § 1-5-621(6), the City and County of Denver ("Denver County") submits this request for reconsideration of the December 17, 2007 decision to decertify the Sequoia Voting Systems Edge II DRE Voting Machines and the Edge II Plus DRE Voting Machines including any and all systems or components associated therewith such as VeriVote; Edge Audio Unit; and Card Activator, Version Number 5.0.31 / 4.4 / 5.0 Rev. C, HAAT Model 50, Version Number 1.2.33. (hereinafter referred to collectively at times as "Sequoia Voting Systems").

In addition, this request for reconsideration pertains to the decision to recertify with conditions other Sequoia equipment or systems including but not limited to the Central Count Scanner (400-c) and Precinct Count Scanner (Insight/Insight Plus), including Memory Pack Reader, Version Number HPXK1.44/APX 2.12, and WinEDS Version No. 3.1.074. The recertification conditions associated with the use of said equipment and systems are constructively a decertification as such conditions are impossible, impractical and unreasonable.

Denver County requests that the Colorado Secretary of State recertify all Sequoia Voting Systems voting equipment and remove or modify all conditions placed on the certified voting systems to allow the Denver County Clerk and Recorder to perform her statutory duties in relation to the 2008 elections. Denver believes and asserts that your decision to decertify Sequoia Voting Systems, including the factors identified in support thereof, was in error or that the deficiencies have been corrected and hereby requests you to reconsider your initial findings and to reverse your decision. In addition, Denver hereby adopts and incorporates by this

reference, in its entirety, the Request for Reconsideration submitted by Sequoia Voting Systems or any other county as additional grounds to reconsider and reverse your decision concerning the Sequoia Voting Systems.

Unavailable Documentation

To date, the only documentation released by your office memorializing the grounds for your decisions on voting system use is the summary document entitled 2007–CDOS-SEQ-001-0403 Sequoia Voting Systems Project Overview and a letter dated December 17, 2007, addressed to Mr. Ed Smith of Sequoia Voting Systems. Although your office previously indicated that affected counties would receive copies of the actual detailed testing procedures, methodologies, analyses, recommendations, and grounds for your decision, such information has not been released by your office.

We are concerned that Denver’s lack of access to all relevant documents may mean that we have not had an adequate opportunity to fully analyze your decision. Therefore, we respectfully reserve the right to edit this request for reconsideration upon the receipt of said documentation.

Statutory Authority to Place Conditions on Voting Systems

While we appreciate the Secretary of State’s efforts to allow the use of certain election systems by placing certain conditions on those systems, we would like to raise the question of whether statutory authority exists to make such conditions as part of the certification process. C.R.S. § 1-5-621(6) grants authority to place conditions for use on a voting system. However, that statute suggests that conditions can only be placed on a voting system in response to C.R.S. § 1-5-621(2), which states “A voting system provider or a designated election official using an electronic or electromechanical voting system shall give notice to the secretary of state within twenty-four hours of a malfunction of its system in preparation for or during an election. The notice may be verbal or in writing. For purposes of this section, ‘malfunction’ means a deviation from a correct value in a voting system.” Since there has been no “malfunction” reported by a vendor or designated election official, it’s questionable whether the Secretary of State has the authority to place conditions on voting systems in this certification process. Therefore, it would be helpful if the Secretary of State’s office could provide an explanation as to how it believes it has the statutory authority to require conditions on these voting systems.

RECONSIDERATION OF DECERTIFICATION OF EDGE II & EDGE II PLUS DRE

The restrictions cited relative to the Edge II Direct Record Electronic (DRE) can be grouped into documentation and functional classifications.

Before addressing those classifications, we wish to address the first two of the three comments regarding the Edge II DREs from your letter of December 17th. In the letter, you describe the primary reasons for decertifying the Edge II as: “Failure for the device to operate in a secured state requiring passwords, and failure to provide auditable data to detect security violations.”

We wish to comment as follows:

1. The FEC 2002 Voting Systems Standards, to which these units are certified at the federal level do not require the DRE to have a password.

2. The audit-related restrictions regarding the Edge II stated in the Test Board report, also dated December 17th, section page 6 references only these two following Rule 45 items:

- 45.5.2.5.3 The voting system shall track and maintain audit information of the following voting system application events:
- Log on and log off activity.

Regarding the comment for 45.5.2.5.3, the Edge II DRE does not provide log on and log off activity monitoring because, as noted, there is no password-related log on/log off capability.

This restriction is thus an obvious cascade from the lack of a password for the DRE. As the voter has no capability to perform administrative functions, and the poll worker has very limited Election Day related maintenance functions, one could argue that a log on capability is unneeded. In fact, the Test Board could have recommended that the jurisdiction secure the unit via a lock and key. Log on passwords and physical keys have the same security-related strengths and weaknesses. Both are given only to authorized persons. Both can be given away by those authorized persons. Both can be lost, requiring the jurisdiction authority to replace the lost physical key or reset the log on password. The Secretary can comfortably and successfully mitigate the concern regarding log on passwords by requiring a lock on the hard shell case of the Edge II. The hard shell case is already amenable to this added physical security.

Regarding 45.5.2.5.5, “If a vote tabulation device employs the use of removable memory storage devices, the devices shall allow for an alternate method of transfer of audit records if the device and/or memory storage device is damaged or destroyed.” The situation that this portion of Rule 45 attempts to mitigate (loss of either the DRE unit or its corresponding memory card) has never been an issue across the over 30,000 Edge II units deployed for many years, some since 2001. The Test Board agreed that if the memory card is lost, its information can be obtained from the Edge II unit from which the information is derived. Of the two possible scenarios, loss of memory cards or loss of an Edge II unit, obviously the smaller memory card is easier to lose. As stated above, the Edge II unit is at present programmed to, and capable of, rectifying a lost memory card situation.

Documentation Related Restrictions

The Test Board cites a number of documentation-related issues regarding the Edge II, as well as other equipment that was conditionally certified. We reject the majority of these comments as erroneous. Three documents were provided to the Test Board, although cited as not having been provided at all. The documents, the applicable Rule 45 clause, and date submitted are (where applicable):

45.5.1.2 All voting system software, hardware, and firmware shall meet all requirements of federal law that address accessibility for the voter interface of the voting system. These laws include, but are not necessarily limited to, (a) the Help America Vote Act, (b) the Americans with Disabilities Act, and (c) the Federal Rehabilitation Act. The voting system provider shall

acknowledge explicitly that their proposed software, hardware, and firmware are all in compliance with the relevant accessibility portions of these laws. Petitioner's (including Sequoia Voting Systems, the manufacturer) do explicitly state that the products submitted for certification do comply with the listed statutes as interpreted through the FEC 2002 Voting Systems Standards.

“Processing Requirements” - Page 4, section title: AVC Edge 5.0; Rule 45 clause: 45.5.2.2.3. The voting system provider shall publish and specify processing standards for each component of the voting system as part of the documentation required for certification; submitted October 5, 2007. Note that this document is cited as lacking across multiple portions of the voting system information submitted.

“3M_touchscreen_film_Edge II” - All pages, but particularly “minimum contact”, “operating temperature” and “humidity” all on page 2; Rule 45 clause: 45.5.2.3.13: All DRE voting devices shall use touch screen technology or other technology providing visual ballot display and selection. The voting system provider shall include documentation concerning the use of touch screen or other display and selection technology, including but not limited to:

(b) Technical documentation describing the nature and sensitivity of any other technology used to display and select offices, candidates, or issues; submitted October 5, 2007.

“Accessibility – AVC Edge 5.0” - Page 3; Rule 45 clause: 45.5.2.8.2 requires Sequoia to provide documentation regarding the “Technology used by the voting system that prevents headset/headphone interference with hearing aids.” Sequoia did place a statement in the referenced accessibility document. Note that federal standards require testing for this to ANSI standard C63.19: “American National Standard for Methods of Measurement of Compatibility between Wireless Communications Devices and Hearing Aids.” This National Standard encompasses both methods of measurement and definitions of limits for establishing hearing aid compatibility and the accessibility of wireless communications devices to wearers of hearing aids. The Test Board should have accepted the statement in the document provided, as Sequoia does not supply wireless headphones or other audio devices.

45.5.2.3.2 The voting system shall meet the following environmental controls allowing for storage and operation in the following physical ranges:

(a) Operating – Max. 95 Degrees Fahrenheit; Min 50 Degrees Fahrenheit, with max. humidity of 90%, normal or minimum operating humidity of 15%.

(b) Non-Operating – Max. 140 Degrees Fahrenheit; Min. 4 Degrees Fahrenheit. Non-operating humidity ranges from 5% to 90% for various intervals throughout the day.

The material supplied by the voting system provider shall include a statement of all requirements and restrictions regarding environmental protection, electrical service, telecommunications service, and any other facility or resource required for the installation, operation, and storage of the voting system. A review of the various Wyle reports (such as report 51884-10 sent directly to the Test Board by Wyle Labs of Huntsville, Alabama) and the Operations and Maintenance manuals for each portion of the voting system (provided at various times from the outset of the certification process through October 7, 2007) discuss and fulfill the requirements stated in 45.5.2.3.2. The humidity requirement is specific to the State of Colorado and given the time to have this tested based on the timelines imposed by the Secretary, should not be considered in the

decision to certify the equipment. Of course, it is arguable that Colorado voting systems need a humidity specification considering the regional climate.

45.5.2.6.3 The voting system provider shall submit to the Secretary of State its recommended policies or guidelines governing:

- (d) Effective password management;
- (e) Protection abilities of a particular operating system;
- (f) General characteristics of supervisory access privileges;
- (g) Segregation of duties;

Sequoia did not provide documentation because, as noted elsewhere in this request, the Edge II DRE does not have a password capability. Nonetheless, as also described elsewhere in this request, the Secretary should certify the Edge II with Card Activator/HAAT50 based on either other mitigations or the lack of need for a password to protect the DRE. The security threat overcome by a password is simply not present.

45.5.2.7.10 Voting systems providers shall document how they plan to monitor and respond to known threats to which their voting systems are vulnerable. This documentation shall provide a detailed description, including scheduling information, of the procedures the voting system provider will use to:

- (a) Monitor threats, such as through the review of assessments, advisories, and alerts for COTS components;
- (b) Evaluate the threats and, if any, proposed responses;
- (c) Develop responsive updates to the system and/or corrective procedures; and
- (d) As part of certification requirements of the proposed system, provide assistance to customers, either directly or through detailed written procedures, how to update their systems and/or to implement the corrective procedures within the timeframe established by the Secretary of State. Sequoia has devised a procedure that will comply with the above requirements and will provide it to the Secretary on or before the Hearing regarding this request.

Similarly, we believe that through other documentation provided by Sequoia and by the federal testing labs, the Secretary's requirement for documentation regarding the Edge II with Card Activator (as well as all other portions of the voting system submitted for certification under this application) is substantially met and met far more adequately so than the Test Board's Report would indicate.

Functional Related Restrictions

Although difficult to assign to a particular restriction as listed in the Certification Report, the Edge II has been cited by the Secretary as having inability to "ensure all electronic records have corresponding VVPAT records." This is the third of the three items on the Secretary's letter of December 17th. The Test Board was later asked about the reasoning for this, and the Board cited the alleged lack of a VVPAT printer test utility when the Edge II is in a polls open status. The Test Board continued to state their belief that the lack of a printer test utility could allow for an undetected improper change of VVPAT paper, leading to improperly printed VVPAT records. As demonstrated by Mr. Ed Smith of Sequoia Voting Systems to members of the Test Board on December 21st, there is in fact a specific procedure and existing programmed capability in the Edge II version under consideration (version 5.0.31 as federally certified) to perform a printer

test immediately after VVPAT paper is changed. This capability mitigates the Test Board's stated concern and thus should not enter into the Secretary's decision regarding the certification status of the Edge II with Card Activator.

45.5.2.6.1 All voting systems submitted for certification shall meet the following minimum system security requirements:

(a) The voting system shall accommodate a general system of access by least privilege and role based access control. The following requirements shall apply:

(vi) Voting system provider shall not have an administrative account, or administrative account access.

(e) The voting system shall meet the following requirements for password security:

(i) All passwords shall be stored and used in a non-reversible format;

(iv) The application's database management system shall require separate passwords for the administrative and each user/operator accounts with access to the application.

(vi) The system shall be designed in such a way to facilitate the changing of passwords for each election cycle.

(vii) The use of blank or empty passwords shall not be permitted at any time with the exception of a limited one-time use startup password which requires a new password to be assigned before the system can be used. These requirements speak to a password protected voting system.

While the DRE unit itself does not have password protection, the WinEDS Election Management System does; therefore, the goal of keeping the manufacturer as well as other untrusted entities from system access is indeed fulfilled. Once again, the need for password protection on the DRE units has not been well articulated by the Test Board, nor does one find a comparable threat in the authoritative literature. Petitioners assert that through the existing system capabilities and the Secretary's traditional election security procedures, security over the voting system (including the DRE units) is quite adequate.

Accessibility: There are several accessibility related citations in the Test Board report. These are:

1-5-704

35.1.5

35.1.6

35.1.8

35.1.11

(1) Notwithstanding any other provision of this article, each voting system certified by the secretary of state for use in local, state, and federal elections shall have the capability to accept accessible voter interface devices in the voting system configuration to allow the voting system to meet the following minimum standards:

(d) Devices providing audio and visual access shall be able to work both separately and simultaneously. *This is not present on the Edge II version 5.0. Version 5.1 does possess this capability.*

(e) If a non-audio access approach is provided, the voting system may not require color perception. The voting system shall use black text or graphics, or both, on white background or white text or graphics, or both, on black background, unless the secretary of state approves other high-contrast color combinations that do not require color perception. *The Edge II is capable of color or black and white (monochrome) display.*

(g) The voting system shall provide audio information, including any audio output using synthetic or recorded human speech or any auditory feedback tones that are important for the use of the audio approach, through at least one mode, by handset or headset, at high volume and shall provide incremental volume control with output amplification up to a level of at least ninety-seven decibel sound pressure level with one incremental level of eighty-nine decibel sound pressure level.

(h) For voice signals transmitted to the elector, the voting system shall provide a gain adjustable up to a minimum of twenty decibels with at least one intermediate step of twelve decibels. *The Edge II meets the Federal standards (FEC 2002) for audio levels. The added requirements are State specific and given the allowed timeframes for certification in Colorado should not be a factor in the Secretary's certification decision.*

(j) If sound cues and audible information such as "beeps" are used, simultaneous corresponding visual cues and information shall be provided. *Petitioners assert that the Edge II meets this criteria.*

37.1.4 The voting systems described in the foregoing paragraphs shall produce a record with an audit capacity for such system.

(d) The paper record shall be accessible for individuals with disabilities including non-visual accessibility for the blind and visually impaired, in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters.

45.5.2.9.10 The V-VPAT device shall be designed to allow every voter to review, and accept or reject his/her paper record in as private and independent manner as possible for both disabled and nondisabled voters. The technology to read the VVPAT to the blind and low vision voter is not federally certified nor does it exist in a manner that manufacturers would be capable of interfacing it to existing DRE units. This requirement should not be a factor in the Secretary's certification decision.

RECONSIDERATION OF CONDITIONS PLACED ON DECERTIFIED SYSTEMS

We ask that the Secretary of State reconsider the following conditions placed on the decertified Sequoia Voting Systems.

Conditions on Edge II and Edge II Plus

1) External Battery Backup (UPS) Devices Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component.

Denver County's Response:

The batteries for the Edge II last two hours, which is the federal testing standards mandate and it is the County's position that the federal standards are sufficient. Power outages are typically far less than two hours; and County Clerks maintain back-up equipment on standby during both early voting and on Election Day. This back-up equipment can be deployed in less than two hours, rendering moot this onerous and non-standard requirement for three hours of back-up

power. Thus, the required acquisition and use of an External Battery Backup (UPS) is an expensive and unneeded condition for use.

9) Device Security Accessibility.

A) The “override.ini” file must not be used with the voting system. The file is not a vstl-approved file, and poses potential for security threat (denial of service in particular).

Denver County’s Response:

The override.ini file is used to allow for non-default language audio and images, typically to meet second (non-English) language and State specific verbiage requirements on the screen display or the VVPAT tape. The County recommends the Secretary allow use of a statewide standard override.ini file. Since the file is a text file, its contents are easily inspected and audited at any place in the election cycle. A standard file allows for the Colorado specific verbiage on the VVPAT tape for the election judge signatures, as well as the fulfillment of Condition 8 for VVPAT review instructions. A standard file issued by the Secretary, and audited during the election cycle, mitigates concerns over its misuse. Sequoia disagrees with the contention that override.ini could be used for a denial of service attack. Furthermore, WinEDS and the Edge II were federally certified with this file included.

9(b) and 10(b) Devices deployed in Colorado shall require a “lockable” activate button. The button shall be protected with a tamper evident seal. This form of activation shall not be used in the voting environment. Only activation by voter access card using the Card Activator as tested.

Denver County’s Response:

The Testing Board’s recommendation suffers from an inadequate definition of the security threat (if any) posed by an exposed Activate button. Denver County would like to have the option to activate the Edge voting machine manually. In Denver County, during the November 2006 Election, voters reported feeling more comfortable watching the judge enter their precinct number manually, as opposed to using the voter card. Furthermore, if there is an issue with the Card Activator or HAAT, Edge machines would be inoperable without the manual activation button. Also, election judges must have access to this button to conduct printer tests when new printers are installed. The activate button can be secured by stationing an election judge behind the voting machines at all time to ensure that no one has access to the activate button.

Alternatively, the button can be sealed with the robust yellow hinged cap supplied by Sequoia. This one piece hinged hard plastic cap possesses an integral loop for use with a wire tamper evident seal (like the seals placed on a natural gas meter). Combined with two-person logging, this solution provides suitable security over the button. If the perceived threat is a voter self-activating the Edge unit and thus voting multiple times, a sealed cap over the button precludes this unlawful behavior. Once again, the Test Board’s recommendation is not supported by a stated or valid security threat to the Edge.

10(c) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to single person entry with detailed logs.

Denver County's Response:

Denver County requests this condition be modified to allow two people access to device level administrative functions. Best business practices and information security practices always suggest having two people have access to secure areas. In fact, ISO27001, the International Standard for Information Security Management Systems, devotes a section of the Standard to "Segregation of Duties" as segregation/separation of sensitive tasks among a small selected group is the best means of securing those tasks. There is no redundancy with single person access. If something should happen to the sole person with access, voting operations could be crippled.

Denver's Suggested Conditions for the Edge II and Edge II Plus

In addition to reconsidering the above conditions, the City and County of Denver would like the Secretary of State to consider certifying the Edge II and Edge II Plus with the following conditions if necessary.

1. The Edge II was submitted to the Colorado Department of State for certification with the Card Activator. If the Edge II is certified upon reconsideration, Denver County requests the ability to use the HAAT50 with the Edge II as well. Three of four Colorado counties using Sequoia equipment already have an inventory of HAAT50s. Each county has used the HAAT 50 with the Edge II in previous elections and have not experienced any issues with the HAAT incorrectly activating the Edge II. The HAAT50 simply activates voter cards by writing the selection code or ballot style number to the voter card. The Card Activator and HAAT50 share the selection code/ballot style format – one could not determine whether a voter card of the same selection code/ballot style came from a Card Activator or a HAAT50. There is no reason to consider the HAAT and Edge2 as incompatible.
2. If the Secretary of State does not approve the Edge II or Edge II Plus machines for use because the existing conditions listed do not mitigate the deficiencies in the Edge II and Edge II Plus voting machines in a satisfactory manner, we would like to suggest a further condition be placed on the Edge II and Edge II Plus in order for them to be used in the 2008 election cycle. In order to provide accessible balloting to voters with disabilities in compliance with the Help America Vote Act of 2002 (HAVA), Denver may use no more than one Edge II or Edge II Plus per precinct on Election Day. Denver may also have one unit available at each precinct for fail-over redundancy purposes.
3. If the limited used stated in Condition #2 above still does not satisfy the Secretary of State's requirements, we would like to suggest that in addition to that condition, that Denver be required to conduct a 100% manual tally of the votes cast on the machines provided for accessible balloting to voters with disabilities. The votes cast would be tallied from the VVPAT provided by the Edge II machines. Alternatively, Denver could be required to duplicate those VVPAT tallies onto regular paper ballots that could then be counted on ballot scanning machines.

RECONSIDERATION OF CONDITIONS PLACED ON CERTIFIED SYSTEMS.

Because the conditions placed on certain recertified Sequoia Voting Systems are impossible, impractical, and unreasonable, such certification is constructively equivalent to decertification. Therefore we ask that the Secretary of State reconsider the following conditions:

Software Conditions

1b) In addition to physical environmental changes, counties shall create a second (or backup) copy of the WinEDS database that is created immediately after the point of memory card downloads. The backup copy shall be stored on close CD Media and documented as matching the master database. This process shall be observed by two election staff members. Chain of custody documents shall be generated for the media, and the media shall be sealed with at least two tamper evident seals stored in a sealed or lockable transfer case that is stored in a limited access area. AFTER the close of polls, the designated election official shall load the sealed copy of the database onto the server and proceed with uploading memory cards after documenting the loading to the backup master database with seals (updating necessary logs) in the limited access location.

Denver County's Response:

While this condition is not unreasonable on its face, in the real world elections environment, it is unworkable. In Denver's central count environment, the time between the memory card downloads and the uploading of the memory cards with election results from mail-in voting is insignificant. This time could be as little as a couple of hours. Consequently, the condition is burdensome and unnecessary. In addition, the physical environment around the server is in strict compliance with SOS Rule 43, which provides adequate security and should mitigate any concerns over a potential "attack" on the system.

We believe there should not be any modification to the server once the election has been set up and memory cartridges have been created. Reinstalling the copy of the database at any time after this point only invites opportunities for error, especially considering all of the circumstances, operations and conditions on election day and night.

However, if the determination is made that more quality control is needed, Denver County suggests moving this process from election night to the time period during the post-election audit, to be completed before the canvass. The escrowed copy of the election database could be loaded on the server and the memory cartridges reloaded at that time, thus duplicating the vote tallying process. This tally could be compared to election night results. Allowing more time for this process would ensure that it is done correctly. It also adds transparency to the process as the canvass board would be able to monitor this process on-site.

1c) Additionally, to overcome deficiencies in security and auditing of the system, the county will be required to perform increased Election Night and Post Election Audits for this system. All post election audit data shall process a hand count of paper ballots which shall match the totals report from the specific device, as well as the totals for the WinEDS database. Counties shall prepare for this event with one of two methods:

Option #1 – Prepare for the upload of memory cartridges as normal. Print necessary zero report. Upon uploading each individual memory card, print a summary report showing the

change in totals from the upload of the memory card. Label the report to match the name/number of the memory card uploaded. Continue to upload memory cards and print totals reports to match. When auditing a specific device, use the difference between the report totals for the memory card selected for the audit and the totals from the immediately preceding memory card report to calculate vote totals generated by the WinEDS software. When memory cards are delivered to the county for upload, the machine generated report shall be delivered for inspection as well. On election night, when the summary report indicated above is created, the difference totals (delta report) are immediately compared to the totals from the report generated by the device at the polling place. If the reports match, the public is ensured that the totals from the polling place match the totals from the county server. If the totals are different, the county is to report the situation (on election night) to the Secretary of State for audit, security and remedy procedures. During the post election audit process, the totals of the paper record for the specific device are to be hand counted and verified against the electronic record for the device. The canvass board shall report the verification of three totals to match – the paper record of the device, the totals of the electronic vote on the device, and the totals in the central count server; **OR**

Option #2 – Prepare for the upload of memory cartridges by creating one master default database (containing all memory cards/cartridges). Create individual databases to contain values (upload data) for each separate memory card (or in some instances by batch of ballots – see condition #4b under Central Count devices. Upload memory card/cartridges into master database, and into the specific database created for that memory card (two separate uploads). This process must happen on Election Night and with observation by at least two people. Election summary reports shall be printed from each individual database and manually added together. The totals from the individual databases must match the master database before proceeding. Upon verification that the master and individual databases match, the county can then use the individual reports to conduct a hand count of the paper ballot (or paper record) generated by the device to show that the WinEDS totals match. The verification of the separate upload databases verify that the database totals match the field totals on each memory card device, as was designed after the point of Logic and Accuracy testing took place.

Denver County’s Response:

The software conditions listed above in conjunction with the conditions listed for the 400-c Central Count Scanner are confusing and poorly written at best and a non-workable, time consuming bureaucratic nightmare at worse. To impose conditions such as these is simply inviting confusion and chaos on election night. Any concerns regarding attacks on the system are mitigated by the physical environment around the server, which is in strict compliance with SOS Rule 43. We are incapable at this time to suggest any new conditions that would satisfy the Secretary of State as his team has failed to adequately explain or demonstrate the alleged weaknesses of the system in the real world.

7) Election Database Creation and Testing. The system relies heavily on an external program called BPS which typically is used for importing the ballot setup process into WinEDS. Since this program is to be considered non-trusted and is not third party as it is made by the voting system manufacturer, the program shall only be able to receive data from WinEDS. WinEDS shall not be used to import data from BPS. Additional testing will therefore be required by counties for both electronic and paper ballots to ensure all voting positions are working as designed prior to each election. This shall include ordering a complete set of at least 5 ballots of each style that contain the prescribed design for that election. County officials shall mark

each possible position for each race on the ballots. All ballots shall be tested internally prior to the public logic and accuracy test. The goal of the pretest is to ensure that all available positions are counting when marked correctly.

Denver County's Response:

1. BPS is a ballot print layout software. Its output is self-evidencing (the ballots) which are heavily checked for quality by both the printer and the jurisdiction.
2. BPS exports only candidate, contest, and geographic information to WinEDS. The machine assignment, all DRE related information, and other election definition must be input to WinEDS by hand.
3. Larger jurisdictions use the export to avoid manual data entry (typing by hand) of the election definition information. Typing in the information is time consuming, prone to error, and creates the need to conduct even more expensive and excessive additional testing.
4. Sequoia Voting Systems has offered to have the code of the export reviewed by a VSTL prior to its use in the August election cycle and to have the report and a copy of the software sent directly to the Test Board for its files to demonstrate that it has no malicious content or would in any manner negatively effect an election.
5. Logic and Accuracy testing is done after the files are imported back from BPS. The Logic and Accuracy testing conducted by each county would catch any issues that may have occurred during the file transfer process.
6. The output from the export into WinEDS is also self-evidencing (reference item 1 above regarding BPS). With the other Conditions for testing all positions in an election, the Secretary has ensured an appropriate quality control point over the import. In addition, there are numerous third party database integrity inspection tools available in the market. These tools provide assurance that the structure of the database is not changed from a "gold standard" database. The Test Board has numerous databases in its possession, covering both General and Primary Elections. These, as are all of its test items, represent a known and tested database structure. Sequoia is willing to provide a resource to assist the Secretary in assessing any database that contains contributed content from a BPS export. This resource would, under State or County supervision, test the database using a third party commercially available tool such as AdeptSQL. Running this sort of test takes less than thirty minutes per database. By running this test at any desired stage of the election cycle, the Secretary is assured that BPS did not in any manner change the underlying structure of the database, only import election definition data. An order for each jurisdiction utilizing BPS and accompanying exports to send a copy of the election definition database to the Secretary, after BPS data is populated, would allow for this analysis. The actual analysis requires less than twenty minutes per database; and for this limited investment of time the Secretary would have full assurance that the BPS data import takes no action against the database beyond its stated purpose of data entry. Alternatively, the Secretary could direct Sequoia or the jurisdictions to have the database tested by a third party, with results sent directly to the Secretary's offices.
7. Denver plans to run a pre-election test deck as well as a post-election test deck. In addition, the State mandates a post-election audit. Therefore, any problems in vote totals that could

potentially be caused by malicious software bugs that transferred from BPS to WinEDS would be caught with these tests and audits. Consequently, this is an extraordinarily burdensome and unnecessary condition that ignores other safety precautions.

Precinct Count Scanner Conditions (Insights/Insight Plus):

2) External Battery Backup (UPS) Devices Required.

Insufficient internal power reserves to sustain minimum 3 hour continuous operation. Counties shall purchase and use an external power supply that meets or exceeds the vendor's recommendation for the component.

Denver County's Response:

The batteries for the Insight and Insight Plus last two hours, which is what the federal testing standards mandate. We submit that the federal standards are sufficient. The acquisition of an External Battery Backup (UPS) for each polling location places a large financial burden on each county.

3) Device Security Accessibility.

a) Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to single person entry with detailed logs.

Denver County's Response:

Denver County requests this condition to be expanded to allow two people access to device level administrative functions. Best business practices always suggest having two people have access to secure areas. There is no redundancy with single person access. If something should happen to the sole person with access, voting operations could be crippled.

Central Count Scanner Conditions (400-c):

1) Intrusion seals for protection of trusted build firmware.

Device has no provision of trusted build verification once installed. Counties will be required to maintain constant seals on voting device memory slot, back panel, and other entry points as indicated. Refer to global condition #5a for ensuring integrity of trusted build.

Denver County's Response:

Once the trusted build has been loaded onto the 400-c scanners, the scanners will be under constant camera surveillance and access to their location will be limited to approved personnel as required by SOS rules. Consequently, the additional requirement of placing seals on the memory slot, back panel, and other entry points is excessive and will make the counting of ballots in a timely manner much more difficult.

4) Audit Trail Information:

b) Counties will be required to perform additional post-election audit functions for the device to accommodate for security deficiencies. In an effort to increase confidence in the recording of votes by the device, the post-election audit shall include a hand count of at least the following amounts of ballots:

Considering the closest race in the election, if the difference between the top two candidates for the race is:

*10% or greater, then hand count 60 ballots for every 10,000 cast;
9.00% - 9.99%, then hand count 65 ballots for every 10,000 cast;
8.00% - 8.99%, then hand count 70 ballots for every 10,000 cast;
7.00% - 7.99%, then hand count 80 ballots for every 10,000 cast;
6.00% - 6.99%, then hand count 95 ballots for every 10,000 cast;
5.00% - 5.99%, then hand count 115 ballots for every 10,000 cast;
4.00% - 4.99%, then hand count 140 ballots for every 10,000 cast;
3.00% - 3.99%, then hand count 185 ballots for every 10,000 cast;
2.00% - 2.99%, then hand count 275 ballots for every 10,000 cast;
1.00% - 1.99%, then hand count 550 ballots for every 10,000 cast;
0.01% - 0.99%, then hand count 1200 ballots for every 10,000 cast.*

The verification of the hand count of paper ballots shall match the totals generated from the WinEDS software as indicated in Software Condition #1c. Counties shall load only the master database from the secured storage location for processing the post-election audit ballots as indicated in Software Condition #1b. Counties shall prepare database and batches of ballots prior to scanning into system (for election results) to accurately generate reports in batch sizes as necessary for the audit. If the county or system is not capable of accommodating the requirement of batch size after the outcome of the election is revealed, the highest percentage of ballots shall be used for the audit process.

Denver County's Response:

Denver County believes this requirement is excessive and expensive. The current post-election audit levels of 5% already exceed the requirements that most other states include in their post-election audit and Denver believes that this existing requirement is already excessive and unnecessary. The proper use of test decks before and after an election make the use of additional manual audits unnecessary. In addition, alternative methods are available for mitigating any perceived security deficiencies. For instance, a forensic snapshot of the election database taken before and after the election could detect any malicious changes made in the system. Finally, this type of burdensome audit does not take into consideration the vast array of security measures used by county clerks and their staffs.

This requirement is also extremely expensive as hand counts are very labor intensive and because human errors many times necessitate multiple hand counts. We estimate that the cost to do such an audit would be \$36,000 in the City and County of Denver in a statewide race where there was a difference is 0.1%, and where 250,000 votes were cast. To perform such task would require 3,000 man hours which translates into a crew of 75 workers working 5 days. Such a use of resources does not seem like a wise use of taxpayer dollars to accomplish a goal that can be achieved through other means.

If the Secretary does intend to implement a statistically based sampling plan, however, then the recommended sample sizes should derive from American National Standard Z1.4 "SAMPLING PROCEDURES AND TABLES FOR INSPECTION BY ATTRIBUTES". By using this National Standard, utilized by the military and other large commercial enterprises for goods acceptance decisions, the Secretary is on firm ground prescribing sample sizes. The sample sizes required by the Master Tables in the Standard (pages 10 and 11) would, for the scenario above, require only 1,250 ballots to be recounted under the tightest normal sampling plan for a 0.40% margin of victory and the 270,000 ballots cited. This is far less onerous than the ballots to be

recounted under the current prescription, which does not cite a source of its sampling tables, nor the level of sampling (relaxed, general, or tightened) used.

6) Device Security Accessibility.

Device level administrative functions requiring access involving the use of keys, memory cards, and passwords must be restricted to single person entry with detailed logs.

Denver County's Response:

The County requests this condition to be expanded to allow two people access to device level administrative functions. Best business practices always suggest having two people have access to secure areas. There is no redundancy with single person access. If something should happen to the sole person with access, voting operations could be crippled.

CONCLUSION

In accordance with the Department of State Procedures and Guidelines for Requests for Reconsideration dated January 8, 2008, Denver preserves the right to submit supplementary documentation for your review at or before the public hearing concerning this request.

Denver County appreciates the efforts of the Secretary of State and his staff in dealing with these complex and difficult issues and we want to thank you for your consideration of the matters set forth in this request for reconsideration.

Respectfully submitted,

Michael Scarpello
Director of Elections
Denver Clerk and Recorder's Office

cc: Stephanie O'Malley