1-6-14 Commission Packet Contents:

1. Meeting agenda
2. Kolwicz comment
3. Branscomb comment
4. Recommendations from previous reports
5. Technology Subgroup draft report
   a. Draft report
   b. System and network guidelines
   c. SCORE end user acceptable use policy
   d. SCORE management acceptable use policy
6. Letter from AG re: Caldara
Notice of Meeting

Colorado Voter Access and Modernized Elections Commission

Date of Notice: January 2, 2013

Date and Time of Meeting: January 6, 2014, 1:00 p.m.

I. Notice of Colorado Voter Access and Modernized Elections Commission meeting
You are hereby notified that the Colorado Voter Access and Modernized Elections Commission will meet to discuss the items listed below.

The meeting is scheduled for January 6, 2014, at 1:00 p.m. in the Blue Spruce Conference Room, located on the second floor of the Secretary of State’s office at 1700 Broadway, Denver, Colorado 80290.

II. Invitation for public comment
All meetings of the Colorado Voter Access and Modernized Elections Commission are open to the public. To submit comments in writing, please call (303) 894-2200 x6318 for email instructions.

III. Meeting agenda
- Review draft reports from committees
- Work on draft of report due in January
- Set date, time, and agenda for next meeting

IV. Meeting materials
All documents and materials for the Commission meeting are available to the public online. To view or download these materials, visit the Colorado Voter Access and Modernized Elections Commission page on the Secretary of State’s website.

V. Broadcast and audio recording of the meeting
To access audio broadcasts of the Voter Access and Modernized Elections Commission meeting, visit the Audio Broadcasts page on the Secretary of State’s website.

VI. Office contact
If you have any questions or concerns, please contact our office at (303) 894-2200 ext. 6318.
January 2, 2013

Dear Rep. Rankin,

You asked my take on the 1303 commission and where it should go. Well, here it is, for what it’s worth.

1. Colorado’s election system laws were poor before HB-1303 and are much worse afterward. To repair them, the public needs to agree on: “what’s needed”, and “how do we get there”?

   If the commission is unwilling or unable to complete these first steps, I would recommend that the commission close shop. It is better that the commission acknowledges that the problems are not being addressed, than it is to give stakeholders the false impression that they are.

2. I believe that the commission is currently on the road to a product that won’t satisfy the public.

   Do you recall the phrase, “If You Don’t Know Where You Are Going Any Road Will Get You There”?

   This phrase aptly describes the commission’s current status. Some members are trying to go one place, others are trying to go another, and they are taking the same airplane. Even more pointedly, the public is not an integral part of the process.

   As I am confident that you know, to make positive progress, the commission must first agree on where it is going.

3. I will summarize the mandatory first steps.

   In designing a system, the first thing that must be done is to specify the requirements of the system. Most people do not intuitively understand what it means to specify, and what is meant by requirements. Colorado suffers because the election system requirements are not formally identified, specified, quantified, and managed.

   We believe that the election system requirements specification MUST:

   A. Be broadly endorsed.
   B. Be based on measurable standards.
   C. Include specifications for the following fundamental requirements:
      - every eligible elector has the opportunity to vote in private
      - no ineligible elector is permitted to vote
      - every eligible vote is correctly interpreted and counted
      - no ineligible vote is counted
      - no vote can be associated with a specific voter
   D. Include specifications for the following functional requirements:
      - Security.
      - Accuracy.
      - Transparency.
Verifiability.
Performance.
Accountability.
Reliability.
Availability.
Cost.
Governance.

4. Colorado’s election laws do not formally address these system requirements, and those it mentions are inadequately addressed. A conceptual model of the election system is desperately needed, and it does not exist.

5. As regards to the 1303 commission, I suspect that commission members do not yet share a common set of requirements identifiers, let alone share the same specification and standard for each requirement.

**Step number one** is to get the commission team to be working on the same problem by developing and adopting requirements specifications. Team members that are not versed in requirements specification methodology may interfere with the work and if so should be replaced or relegated to support roles.

**Before embarking on further tasks**, it is vital that requirements be formally adopted. All stakeholders, including the public, must have a fair opportunity to influence the final requirements specifications.

As an aside, the work needed to fix the election system is **systems design work, not political work**. It is important that systems designers, not politicians and/or lawyers, control the work product.

I hope this response is useful to you. I very much appreciate your asking -- very few legislators do. I am available to discuss.

Let me add; I am very grateful to you for the work that you are doing on election integrity. If there is anything that I can do to help you, please let me know.

Yours,

Al Kołwicz

Colorado Voter Group
2867 Tincup Circle
Boulder, CO 80305
303-499-9527
Al@alkolwicz.net
From Harvie Branscomb 1/3/2014 4PM
To the Colorado Voter Access and Modernization Commission, aka 1303 commission:

Sadly the legislative commission tasked with correcting irregularities in implementation and mistakes in drafting of the 1303 bill is proving itself incapable of the task. I was told before HB 13-1303 bill passage that any problems with the bill would be worked out by this bipartisan commission. Few if any of the many helpful ideas and warnings about 1303 provided by citizens and SOS were heeded in the form of constructive amendments. Now these problems must be addressed either administratively here, or eventually and most costly and inconveniently in the courts. The remedies are basically and substantially up to this commission to find and propose for enaction.

I can see zero evidence that constructive improvement will occur from the work of the commission and lots of history already has been recorded to support a pessimistic expectation. In particular the dialog at the previous meeting demonstrates that the Commission is unable to address reality and quite well equipped to create its own version of reality. The sky is described as yellow indeed.

In particular this commission is so mired in the deep ruts of partisan political conflict that it cannot perceive non-partisan election reform advocacy when citizens are offering the makings of a paved highway to a better place.

Now is the time to reverse course, get out of the partisan rut and begin to to the job that the legislature and the people of Colorado expect of you.

Here in another attempt to help I continue to provide public comment in the form of problems with 1303, mail ballot procedures and same-day-registration-tabulation processes in Colorado and possible solutions for same.

Problems with 1303/mail ballot/ same day registration-voting-tabulation and solutions for these problems:

P1 insufficient information collected for eligibility determination- harmonization of deadlines insufficient

S1a CDOR form must be updated to include date of recent move, prior address as of 30 days before election if a new registration, a precise inclusion of the date of election day, and explanation of what precinct means if the word is to be used.

S1b OLVR form must be updated to include date of move, prior address within 30 days
of election day if new registration, and specificity about date of election day. Also must inform the elector if a registration change will not take effect prior to election.

S1c Paper voter registration form must collect the previous address if voter is newly registering or changing address during the 30 day period before an election day.

P2 unclear how to harmonize different residency requirements since under 1303 cannot vote in old district

S2a rules must specify if a proliferation of ballot styles are to be used to solve differential eligibility by district. Even if the local district attempts to harmonize with 1303 by using state deadlines of 22 days residency, voters already live in election districts when newly registering. Only if the deadline is "registered for 22 days" contrary to 1303 does the harmonization work. Consider the case of a new voter who does have residency in Colorado for 22 days but not in a local district for 22 days who will require special handling. And resident of Colorado who is a new registrant who has moved within 22 days of election day but has lived previously in a local district may be eligible for some local districts and not others. Only if zero day residency is agreed to for all election districts will the 1303 based residency format be harmonized in its current form. It is highly unlikely that this will be agreed to.

S2b If a proliferation of ballot styles is to be required, the additional cost and bureaucratic overhead of this will need to be addressed. Every county will have this issue even if they have not yet experienced the controversy as Broomfield has. Each ballot style will exponentially increase in number as each local district with a unique residency requirement is added to the ballot. Coordinated election officials must be given the right to decline to coordinate under these circumstances to avoid excessive ballot styles and confusion.

S2c If some kind of documentary affirmation of residency is being used, the text of the affirmation must be approved in rules and written such that it addresses all cases of residency including prior residence in each affected district.

P3 no feasible way to oversee or challenge same day registration and voting particularly because Colorado tabulates an extraordinarily early 15 days before election day

S3a at least two day grace period between receipt and tabulation of any ballot subject to recent registration change to allow challenge if changed registration or residence necessitates a different ballot style be used

S3b daily publication of a list of new or changed registrations listing the date the grace period will end and tabulation will occur. This provides a functional opportunity for watchers to make informed election challenges.

S3c shorten the period allowed for pre-election day tabulation so that effective watching is possible and the risk of revealing accurate incremental election results is reduced
P4 law insufficient to allow effective challenge of either eligibility or signature

S4a new registration documentation must be available to officials and watchers when eligibility check of envelope is underway, including any ID provided as part of documentation

S4b allow eligibility challenge or signature related challenge both before and after election judge adjudication and always well before separation of ballot from envelope. There should be no time pressure from judges about impending separation that makes an obstacle to challenges

S4c allow challenge of election judge rejection of either eligibility or signature

S4d allow escalation to a higher authority of any challenge that has been rejected by election judges. Such a higher authority might consist of a vote of all assembled election judges while partisan balance is maintained. The due process for this escalation must be provided in rule.

S4e when an envelope is challenged, each contest on the presumed ballot style within should be separately evaluated for eligibility for residency concerns (a result of 1303)

P5 law insufficient to allow challenge of elector using wrong ballot style- either by mistake of officials or by intentional or unintentional action of the elector

S5 require election judges to check the ballot style of received mail ballot envelopes against the actual style on the ballot as reflected on the stub or ballot in a manner that allows confirmation by watchers that the voter returned the style containing 100% of eligible contests.

P6 law does not consider how to treat ballot envelopes that do not contain evidence of identity other than signature (unlabeled envelopes or envelopes with label removed)

S6 require election judges to access the stub of the ballot in unlabeled envelopes to determine the identity of the elector who was issued the stub. SOS rules can provide for adequate voter privacy for this operation.

P7 Statute allows for no stub needed when ballot on demand is in use. Free distribution of ballot on demand printers to each county and time pressure on printing by press and cost of unused ballots all encourage use of ballot on demand. BOD has many integrity issues including privacy violation of ballots that are printed in a way distinguishable from the bulk of ballots.

S7 Ballot on demand printers are capable of printing with stubs and should be required to do so. Ballot on demand ballots should be required to be indistinguishable from all other printed ballots.

P8 Neither law nor rule specify how to selectively count particular eligible contests on a returned ballot. Current practice typically involves duplication and marking the original and duplicate
ballot with a common identifying number. This creates a serious privacy issue by rendering the record of voter intent unique and is a violation of the Colorado Constitutional requirement of anonymity of the ballot. Such a ballot is identified on a duplicate ballot log and is made more unique by the selective removal of marks from specific contests. In addition to the relative uniqueness of the original style, the duplicate ballot with missing marks is rendered in many cases if not most, non-anonymous and therefore in violation of the CO Constitution.

**S8** Instead of selectively duplicating the ballot for purpose of adding votes to the count, a special second ballot for each voter should be marked that contains ineligible votes to be subtracted from the count and neither original nor negation ballot must have any identification of the voter. These special negation ballots may be pre-printed to contain contests from all ballot styles and can be hand or machine counted together post-election and their aggregate count subtracted from the official election results by ballot style by manual entry in the EMS. Of course these special negation ballots are kept separately so that they may be accounted for and also audited. By this method the original ballot is handled in a way indistinguishable from all others and simple duplication errors do not exist.

**P9** Law and election rules are insufficiently clear about the responsibility and authority of election judges and not staff or county clerk to be making decisions about eligibility of returned ballots in envelopes from the moment that the election record is cast and first seen by the county. Current practice sees staff acting in lieu of election judges placing incoming documents into storage locations or logging envelopes into SCORE batches that prejudice their later handling. Handling of ballots that arrive after 7PM but from other election jurisdictions are an example of this lack of clarity.

**S9** Law must specify a standard practice for handling all ballots and related election documents (affirmations, affidavits, IDs, etc.) in such a manner that properly constituted and credentialed election judges make all the decisions regarding eligibility of each envelope and other form of return such as UOCAVA. All incoming envelopes including those to be processed that arrive after 7PM election night must be processed equally by election judges and provided the cure process on a timely basis. An expedited and enhanced treatment is required for notification of those electors whose envelopes are not signature checked in time for the 2nd day deadline after election day for sending the cure affidavit. A cutoff date and time for late processing of these incoming ballots must be determined in law or rule and other handling practices specified. A similar approach must be developed for UOCAVA electors whose return ballots may arrive 8 days after election day. These too must be given the signature discrepancy check and opportunity for a cure process. The 8 day return deadline should be reconsidered or harmonized with the cure process.

**P10** New canvass board rules prevent the canvass board from engaging in activities pertaining to election judges, while staff often serve in functions that should be provided by election judges. Signature discrepancy check is one area where this inappropriate mixing of roles is most apparent.
S10 Make sure that rules make clear that election judges and the canvass board are the only persons responsible for making decisions regarding eligibility or voter intent capture and resolution, rather than staff. Rules must allow canvass board to revisit eligibility issues during a recount.

P11 The signature cure affidavit is dense, confusing and easily misunderstood and improperly filled out. The actual affirmation that "I returned my voted ballot" is virtually meaningless and insufficient for the task. The elector has no idea what signature is on the envelope for which they are presumably affirming the credibility. The signature on the affidavit is not deemed necessary to check under current SOS advice to the counties.

S11a The unsigned affidavit provided to the elector under the requirement to cure should include a printed facsimile or image of the signed ballot return envelope under consideration so the elector may affirm that this particular signature already deemed discrepant i.e. the one that triggered the need for cure is the one being addressed in the affidavit.

S11b The affidavit should not contain a confusing checkbox that might not be checked by mistake.

S11c The affidavit should contain the following affirmation or one of similar effect: in place of "I returned my voted ballot" substitute the following: "I signed the ballot return envelope shown in the attached image, and I also personally marked the ballot contained within."

S11d The SOS should produce rules that require election judges to reply to an elector who has returned the affidavit to the effect that if the affidavit is deemed technically deficient, such as the image of the ID is unreadable the elector may substitute a compliant affidavit.

S11e Signatures on the affidavit affirming the above statement should be compared to signatures available on SCORE and any obvious discrepancy handled by escalation and notification of the DA.

P12 The audit rules post 1303 require that counties operate under the presumption that all optical scanners are central count. The rules for central count, contrary to the statutory requirement, require a sample of ballots to be recounted both by machine and by hand and the two results compared. Statute requires that original election tallies be audited against a hand count. The current rule does not describe an audit.

S12 The SOS can be instructed to conform the audit rules to statutory requirements where feasible. CO counties such as Broomfield, Eagle and Pitkin and Boulder arrange for original election tallies to be of auditable scale. UVS might eliminate this defect in voting systems functionality that makes it difficult to audit original election tallies when large numbers of ballots are being processed together, but before UVS is a reality we do not need to abandon the already limited accuracy of our pre-1303 audit.
Likewise the Colorado recount is rendered ineffective when it attempts beyond all reason to replicate the limited accuracy of the original election count by replicating all procedures except the use of a review of undervotes.

The recount statute can be brought into the current century by recognizing the function of the recount is not to achieve a perfect replica of the original count but rather to ascertain to the maximum accuracy possible within reason the correct results obtained from evaluating the voter intent on every eligible ballot and no ineligible ballots including evaluating some or all by hand.

A particularly convincing recount can be obtained by sorting the ballots to be recounted by candidate or contest choice first before machine tabulation, such that each tabulator or memory card counts only ballots that have been sorted for a particular choice of the voter, such as "Yes". When this simple review of voter intent is done to separate the ballots before machine counting on separate tabulators, every discrepancy in voter intent capture is likely to be discovered and reconciled in a very efficient way. It is hard to imagine a further dispute of a recount performed this way in the presence of watchers.

SCORE is being used in non-standardized ways to account for elections. Registered electors appearing to vote, Cast Ballots and Votes Counted are three separate entities that must be accounted for separately. It is not clear that SCORE is programmed in a way sufficient to collect the necessary data. Observation suggests that SCORE is not adequately programmed to track and record the provenance and history of each incoming ballot envelope and other valid container and source of incoming election record. Not just ballot envelopes, but also IDs and affidavits and affirmations must all be tracked for accountability. Stubs allow for one stage of ballot tracking but are largely not being used for this purpose. Most problematic is the use of the "accepted" and "rejected" flag in SCORE and use of particular batch identities to predict or prejudice the decision of election judges. This kind of misuse of these flags will make misleading information available to electors who attempt to learn of ballot status from sources that are based on SCORE data.

An evaluation of actual business practices with SCORE in each county is needed to harmonize and rationalize the practices.

Harvie Branscomb
970-9631369
harvie@electionquality.com
[these pointers to access me are released for use in the public record, HB]
CVAMEC Recommendations from Previous Reports

Needs Assessment of the Current State of Voting & Registration System Technology
July 15, 2013

Needs for 2013

• Develop uniform business process to operate VSPCs
  o Requires technical changes to the Citrix modules within SCORE
• Promulgate rule changes required to implement HB 13-1303
• Design and implement modifications to the Voter Registration and Early Voting modules in SCORE to support the VSPC business processes and VSPC functions required by HB13-1303
• County users must be trained to follow standardized VSPC operations
  o A training plan needs to be finalized, a program developed and delivery accomplished.
• Analyze whether available throughput is adequate and options available to increase throughput should be explored
  o Estimate number of users and transactions
• Information system security analysis - in order to ensure that each VSPC is adequately covered by security procedures and is in compliance with applicable standards
  o Determination of whether COCS standards apply to operating VSPCs & VSPC access to SCORE
• Policy decisions must be made to determine which processes should be uniform throughout the counties and which may be developed independently by each county
  o Current processes that may require modification include, but are not limited to, sending confirmation cards to voters, enforcing registration deadlines, reinstating voters to an active status, assigning inactive status, handling cancellations, and producing reports
  o New processes include, but are not limited to, handling requests for email communications, enforcing the twenty-nine day deadline to change or withdraw affiliation, processing NCOA lists, and providing the location of the nearest VSPC on the voter information card.
• Online Voter Registration web application must direct any voter attempting to register or update their residential address after the eight day deadline for new registrations and residence changes has passed to visit a VSPC, PMIV must be removed and all required questions and the affirmation must be included in the module
• Modify the forms used to register voters at DMV facilities to include the changes required in Section 14 of the Act
• Develop and implement a process to update IFTP to active status
• Change voter history report generated by SCORE to add “Mail Ballot” and “VSPC” and removed “Early Voting”, “Mail-in Ballot” and “Polling Place”
• Plan, develop a set of procedures, and monitor the VSPCs to ensure that all of them are compliant with the Federal “Americans with Disabilities Act” (ADA) of 1990; new and existing facilities and equipment should continue to be evaluated and appropriate caution should be taken to mitigate the risk of non ADA compliant sites
• Procedures must be developed and resources provided to support any emergency relocation of a VSPC and reestablishing its connectivity to SCORE
• Negotiate agreements with Vital Records and Corrections to provide daily updates during the fifteen days prior to and on Election Day

Needs for 2014

• Secured web applications to support the operation of the VSPCs must be developed for SCORE to create a more streamlined and integrated process for users. These applications need to have a capacity sufficient to support the sheer number of physical locations, users and transactions necessary to conduct the 2014 elections. These applications should be tailored to suit the needs of the uniform business process being developed by the counties and CDOS. The secure web application must access the critical SCORE functionalities that have been enhanced allowing users to continue to provide services in the VSPCs to:
  o Serve all voters in the county.
  o Access the statewide voter registration rolls through a secure connection.
  o Register new voters
  o Check voter eligibility
  o Update existing registration information
  o Allow an unaffiliated voter to affiliate with a political party and cast a ballot in a primary election
  o Issue and receive mail and provisional ballots
  o Issue replacement ballots
  o Support printing ballots on demand
  o Record ballots cast in person, both on paper and on Direct Recording Equipment (DRE) voting devices, within the VSPC

• SCORE also needs to be modified to support county election offices in functions outside of the VSPCs including:
  o New functions:
    ▪ Record voter requests for e-mail communication, or reversal of such requests
    ▪ Recognize undeliverable e-mail messages and send the undelivered as well as any future communications through the United State Postal Service.
    ▪ Protect voter email addresses from unauthorized disclosure.
    ▪ Maintain a record of all correspondence sent to an elector in the elector’s record under subsection 1-1-110(5), C.R.S.
    ▪ Email communications will be part of the county business process and records of that process are to be maintained on SCORE. Although the Act does not require the email communications from the counties to the voter to be integrated into SCORE, the required record keeping would be most efficient if the emails were managed by the county through SCORE. The Business Practices Subgroup should evaluate this as they develop the business process.
  o Modification to existing functions:
    ▪ Enforce the multiple voter registration deadlines
    ▪ Enforce the twenty-nine day deadline for changes or withdrawals of affiliation
    ▪ Enforce the new state residency deadline

• Assess usability and efficiency of the county business process and uniform VSPC business process to identify parts of the business processes that worked and those that need improvement for 2014
• Analyze adequacy of system throughput for 2014, taking into account number of VSPC locations, plans for equipment and staffing levels, estimated turnout, voting patterns and system loads experienced during 2013. The system should also undergo load testing to ensure that SCORE can handle the number of county users and increased system workload anticipated in 2014.
• Explore the feasibility of fully integrating the NCOA process into SCORE, including providing match data to the counties and generating the required mailings of voter confirmation cards in SCORE
• Explore feasibility of acquiring data differentiating mailing, residential and temporary address changes

Assessment of Voting System Technology Report
August 30, 2013

• Over half of Colorado’s counties will need to replace their voting systems within the next 5 years due to end of life
• The next generation of voting systems within Colorado will need to provide a ballot marking device, optical scanner, DRE and high speed central count scanner, at a minimum
• As the mail-in election model matures within the state and the percentage of ballots cast via mail normalizes, consideration should be given to how the overall cost may be affected by actual usage patterns during elections
• Costing estimation should take into account the cost of each hardware device, the software of the voting system as well as any third party applications not included with the voting system itself, and support and maintenance costs for each applicable component of the voting system
• Develop a well-defined criteria list prior to selecting a UVS system, including reporting flexibility, ease of use of each component, maintainability, sustainability, types of voting equipment supported, and flexibility of the system to accommodate new technologies
• The state should implement a sufficiently staffed technical group that will be able to assist the counties when technical issues (UVS)
• The State will need to look for ways to fund the UVS initiative in order to assist the counties as much as possible
• A UVS system must be flexible and not overly dependent on proprietary hardware
• UVS implementation should be phased to build upon success and to accommodate the needs of all counties
Prepared for consideration for inclusion in the Commission report due January 15, 2014

Report of the Technology Subgroup of the Commission, prepared by Trevor Timmons, CIO for the Secretary of State’s Office

Background

With the adoption of HB 13-1303, the department moved to implement short-term changes to the SCORE system for elections in late 2013. Rules governing elections were adopted on an emergency basis on October 9, 2013, for Coordinated Elections in November 2013, and minor modifications to the SCORE system were made to allow the conduct of elections in accordance with statute and rule.

The department worked closely with the commission established by 1303 to complete two reports for the General Assembly, with a third report due on January 15, 2014. The reports identified 61 areas for consideration of impact to SCORE and the conduct of elections arising from 1303. Sixty-two percent of the items have been addressed either through software changes to SCORE or the department’s online voter registration system or because they required county business process changes, not software solutions. Twenty-two areas—36 percent—will be addressed through future software changes or business process changes. The Commission is monitoring the work of the department and county clerks to ensure that the requirements of 1303 are fully met.

Four key areas are expected to be the focus for work by the Technology Subgroup of the Commission in 2014 in collaboration with the Business Practices Subgroup.

Systems

In the elections domain, an “electronic pollbook” refers to the system or process of verifying voter eligibility and tracking election activity of registered voters through network-connected, real-time access to a state voter registration list. The ability to verify eligibility of potential voters, add eligible electors to the statewide list, and issue the appropriate ballot at a VSPC is critical to maintaining the integrity of elections. The department considered three approaches to meet this need:

Option 1: Minor Modifications to SCORE’s Early Voting Module:

One option is making simple modifications to the SCORE early voting module and planning to utilize it for VSPC operations. This was essentially the approach used for recall elections in September 2013 and the 2013 November Coordinated Election. Based on the number of voting locations required under law and historical data on voter turnout for a statewide coordinated election, this method was deemed appropriate. And the suitability of this approach for the Coordinated Election was proven.
This approach is likely also suitable for the Primary Election in 2014. Again, based on the number of voting locations required under law and historical data on voter turnout, this method would likely prove sufficient.

For the 2014 General Election however, this approach is likely to face shortcomings. Based on the number of VSPCs that will be required for a General Election (approximately 260), along with normal back-office mail ballot processing, the department estimates that an additional 1,000 to 2,000 Citrix user licenses and server infrastructure to support them would be needed. At an initial cost of approximately $250 per license, not including infrastructure improvements, this option could cost the Secretary of State at least half a million dollars without modernizing the core SCORE application. The department deemed this the least attractive of three options.

Option 2: Purchase a commercial off-the-shelf electronic pollbook and integrate with SCORE for VSPCs

The department posted a Request for Information to determine whether some of the commercial options appeared suitable for use in servicing VSPCs. After reviewing responses to the RFI, they posted a Request for Proposals for a statewide electronic pollbook. Six companies responded to the RFP.

The cost proposals ranged from approximately $900,000 to $3.55 million. After a review of all six proposals and oral presentations from the vendors, the evaluation committee recognized that all the products would require significant customization to meet Colorado’s requirements. The evaluation committee unanimously agreed that none of the six proposals were suitable for selection. This option was deemed unacceptable due to the cost of acquiring a commercial e-pollbook system in addition to the risk and extent of the modifications that would need to be made to all of the available products.

Option 3: Build a secure, web-based application to meet VSPC needs for Colorado

After assessing the commercial market, the department is proceeding with a “build” project, to create a secure web-based application for use in voter service and polling centers (VSPCs). This project is being managed by the department, and will involve the use of contract software development resources in calendar year 2014. The department is working with Colorado County Clerk and Recorders to finalize requirements and functional specifications by early February 2014.

An electronic pollbook needs to be tested to ensure it will meet the transaction loads expected of it. Performance and stress testing, in conjunction with county training and mock election activities, will help identify the limits, if any, that may constrain counties in planning for VSPC operations in 2014 and beyond. Performance testing should also show whether the department needs to look to private or public cloud options to deliver VSPC functionality across the state at peak times.
Security

Historically, less than a third of Colorado counties have used electronic pollbooks on Election Day. Extending the window of time during which counties are accessing the state registration list, and expanding the number of locations from which this access is needed requires thoughtful analysis and more robust security measures.

The department is working with the Governor’s Office of Information Security to identify and put in place more effective controls, systems, and policies for voter service and polling centers (VSPCs). Some of the areas under consideration are:

- Developing guidance for counties to consider as they are preparing for extensive use of VSPCs that must have reliable, secure connections to the statewide list of registered voters for normal operations (a draft guidance document has been included with this report as Appendix T-1);
- Implementation of more sophisticated cybersecurity systems (e.g., web application firewalls, advanced persistent threat prevention systems, endpoint malware detection systems);
- Expanded use of the multi-factor authentication system already in use for full-time county elections staff to temporary election workers; and,
- Revision of policies governing use and access to state voter registration systems (draft policy documents have been included with this report as Appendices T-2 and T-3).

The department is currently preparing a needs and risk assessment of SCORE and the planned web-based applications for use in VSPCs to inform security-related enhancements for SCORE.

Data and Data Interfaces

Timeliness of data for voter verification and eligibility checking is an important component of 1303. Statewide use of National Change of Address (NCOA) information and improving the timeliness of death and felon data used for verification are key areas for improvement.

The Technical Subgroup believes an assessment of the timing and utility of existing data interchanges based on findings from the 2013 elections would be useful. If existing data comparisons and the frequency with which they are performed could be improved, a concrete plan for improvements should be created. If the existing methods are suitable, the state and counties should validate that they are sustainable and continue to monitor them for success.

Technical Logistics

By eliminating a deadline for voter registration, 1303 has brought about a need for real-time access to a dynamic statewide voter list at every voting location. Counties that have historically conducted elections by means of precinct-based locations using paper pollbooks now must secure and prepare locations
where voters, or prospective voters, can change their registration or register for the first time and cast a regular ballot. Counties that have experience with vote center elections face the least change, but they must still prepare for handling new registrations, and more mail-ballot drop-off options than we have seen previously in Colorado.

Addressing some of these needs will require technical solutions, but many will be solved through changed business processes and practices. Some areas for consideration as counties are planning for VSPCs are:

- Where did counties add VSPC locations in 2013, and where will they need to add for 2014?
- What infrastructure needs will counties have to meet for VSPCs in 2014?
- Will any VSPC locations require wireless connectivity? Do counties need assistance finding secure wireless connectivity options?
- What needs will counties have to meet for secure workstations or devices deployed at VSPCs? Do counties need assistance finding secure endpoints for use in VSPCs?
- Should counties consider setting up 24x7 mail ballot drop-off locations if they have not in the past? What do counties need to do to properly secure 24x7 drop-off locations, and do the benefits outweigh the costs?
- Can counties monitor VSPC locations well enough to shift resources from one location to another during voting if warranted?
- Can counties prepare models for planning purposes to assist with handling election turnout?

**Risk Register**

The department and the Commission have agreed to create a risk register to monitor the implementation of 1303 during 2014. This register is intended to guide the department as efforts toward long-term sustainability of 1303 continue. The Risk Register is attached to this report as Appendix T-4.
County Systems & Network Guidelines for SCORE Access

Purpose
These guidelines are meant to help counties meet Federal, State, and Local SCORE systems security requirements. Under each heading are questions that the county must use to analyze their network security. A county has a security problem if the county cannot answer a question or cannot provide an affirmative answer to the question. A county must work with their information technology department to remedy an existing problem.

General
- Do you have an inventory of all devices permitted to connect to the SCORE network?
- Have you performed a site survey to determine what areas within the area need coverage?
  - Are monitors displaying sensitive information blocked from view by the public?
  - Are network ports, network equipment or other systems in non-monitored areas restricted from access by the public?
- Have users been trained to never post or store passwords, grid cards, wireless keys or other sensitive information on or around work areas or workstations?
- Are network ports and/or wall jacks monitored and/or restricted from public or other non-county related use?
- Is access permitted to only known trusted DNS servers?
- Are vendor supplied defaults for simple network management protocol (SNMP) community strings and passwords changed?
- Is all non-console administrative access encrypted using technologies such as SSH, VPN or SSL/TLS?
- Are all system changes go through a County IT management change approval process?
- Are proper security controls in place to monitor physical access to SCORE systems?
  - Do you have staff monitoring, cameras, locks or other controls needed to ensure only authorized personnel can access networks and systems?
- Are all authorized staff required to wear identification, such as a government issued photo ID badge, to clearly distinguish between onsite personnel and public visitors?

Network
- Are all network devices including firewalls, routers and switches configured according to industry best practices?
- Is there documentation and business justification for use of all services, protocols, and ports allowed?
- Are firewall and router rule sets reviewed at least every six months?
- Are network ports and/or wall jacks monitored and/or restricted from public or other non-county related use?
- Is access permitted to only known trusted DNS servers?
- Is there an up to date network diagram including any wireless networks?
- Are vendor supplied defaults for simple network management protocol (SNMP) community strings and passwords changed?
- Is all non-console administrative access encrypted using technologies such as SSH, VPN or SSL/TLS?
- Is all network equipment configured to keep accurate time synchronization with a trusted NTP time source?
Wireless Networks

- Do you ensure that all wireless access points are managed by either the State or Counties?
- Do you ensure that all wireless access points are physically secure and not physically accessible by the public?
- Do you ensure that all wireless traffic utilizes at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection?
- Do you disable peer-to-peer wireless network capabilities on wireless clients?
- Do you disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need?
- Do you configure all wireless clients used to access private networks or handle organization data in such a way that they cannot be used to connect to public wireless networks or any other networks beyond those secured and controlled by either the State or County?
- Do you ensure that wireless keys and network information isn’t shared with staff or others that don’t need to know?
  - Do you document all staff that has access to a wireless key or other network information?
- Are wireless passwords and pass phrases changed at least every three months and every time someone with access to the password or pass phrase leaves County or State employment?

MiFi Networks - Cell Phones and Mobile Device Hot Spots or Cards

- Are vendor supplied default passwords and PSK passphrases changed to meet wireless network minimum requirements? Vendor supplied default should never be used!
- If a wireless “Hot Spot” is utilized on a MiFi device are all the wireless network requirements above being implemented?
- Are mobile devices being utilized for MiFi access secured with at least an 8 character passcode meeting password complexity requirements to prevent un-authorized access?

Client Systems – County Workstations

- Do you have an inventory of permitted software applications on client systems?
- Are only software packages needed to perform business related functions being installed?
- Are basic users given non-administrator accounts with no rights to install software on client systems?
- Do client systems have up-to-date anti-virus installed with real time scanning enabled?
- Do client systems have a software firewall installed, configured and enabled?
- Are users restricted from disabling anti-virus and firewall software?
- Do you run a vulnerability scan on client systems? Are vulnerability scans completed on a regular basis or whenever significant changes occur on systems?
- Are all client systems configured securely according to industry best practices?
- Are local administrator privileges controlled and only used when necessary on client systems?
- Are all systems patched with updated operating system and third-party security patches?
- Is any sensitive SCORE data downloaded from the system only stored on securely encrypted drives or devices?
- Do client systems have proper security logging enabled to identify user authentication events, accurate date and time, successful and failure events?
- Are client systems configured to keep an accurate time with a trusted NTP time source?
User Training & Requirements

- Have users reviewed and signed the SCORE Acceptable Use Policy?
- Have users been informed to never share passwords or grid card information?
- Are all users given a unique username before allowing them access to SCORE?
- Are all users required to use a multifactor authentication device such as a grid card or token?
- Are users trained on complex password requirements in the AUP?
  - At least 8 characters
  - Lower-case letter
  - Number
  - Upper-case letter
  - Symbol
- Are users trained on whom to contact if they are experiencing unusual workstation activity?
- Have all County User Administrators completed the Securing the Human course provided by the Colorado Department of State?
- Are users trained to never install software or browse the Internet on SCORE client systems?
- If a user session is idle for more than 15 minutes is the user required to re-authenticate or un-lock their workstation?

Resources for Counties

2. Multi-State Information Sharing and Analysis Center cyber security guides for nontechnical managers.
   [http://msisac.cisecurity.org/resources/guides/](http://msisac.cisecurity.org/resources/guides/)
3. Secunia Online Software Inspector (OSI) – Workstation Vulnerability Scanner
4. Center for Internet Security Hardening Guides
5. SANS 20 Critical Security Controls
6. TrueCrypt Free Encryption Software
7. Online File Malware Checker
   [www.virustotal.com](http://www.virustotal.com)
8. NIST – National Institute of Standards and Technology Publications
   [http://csrc.nist.gov/publications/PubsSPs.html](http://csrc.nist.gov/publications/PubsSPs.html)
SCORE
End User Acceptable Use Policy

PURPOSE:
The SCORE system maintains sensitive information that requires protection. This policy establishes a standard to protect sensitive information contained in the Colorado Department of State SCORE system.

SCOPE:
This policy applies to any person who accesses or uses the SCORE system and any associated equipment that is used to manage, access, and or monitor the SCORE system. All Colorado SCORE users must sign and agree with this policy. [Reference Colorado Information Security Act (C.R.S. 24-37.5, Part 4) and State of Colorado Cyber Security Program P-CCSP 001, dated December 20, 2006]

INDIVIDUAL RESPONSIBILITIES:
An individual accessing the SCORE system must comply with the following standards and provisions:

- Users are strictly prohibited from sharing passwords or multi-factor-authentication devices including grid cards or tokens.
- User’s complex passwords must:
  - Be at least eight characters in length.
  - Contain three out of the four following items:
    - Lower-case letter
    - Upper-case letter
    - Number
    - Symbol
  - Does not contain the user’s name or username.
- Users must avoid passwords that utilize simple dictionary words. Passwords should be generated from pass phrases that are not written down and are easy for the user to remember.
  - Example: The lazy dog was under the porch this morning! equates to “TlDwutm!”
- Users can access, use, or disclose sensitive information only when necessary to perform a job duty. These actions must be expressly authorized.
- Users may not display or provide sensitive information to unauthorized persons. This rule applies to Social Security Numbers contained in document images on workstations, and to other personal and confidential information, such as Date of Birth, Driver License Number, etc.
- Sanctioned SCORE system users must ensure proper workstation management and configuration. As responsible parties they must:
  - Only access SCORE on systems that are managed and controlled by the County or State. Users may not utilize a user-owned device to access SCORE.
  - Ensure sensitive information is not displayed on a computer screen so that unauthorized persons may view the sensitive information.
  - Ensure their screen is locked to prevent access to SCORE whenever they leave sight of a terminal.
  - Practice safe-surfing habits. A user may not casually browse the internet on a system utilized to access SCORE.
  - Not install or download any software including shareware, freeware, or browser controls unless authorized to do so.
  - Harden all systems to meet industry best practices. Center for Internet Security requirements and other vendors such as Microsoft have published hardening standards for individual operating systems that are updated regularly.
  - Contact the SCORE help desk immediately if a system’s performance becomes erratic, or if it appears the system has been tampered with, or the local virus protection software finds an infection. Degraded system performance or erratic behavior may indicate a Malware infection such as a virus or Trojan.
  - Only connect to county controlled networks with proper network security controls in place. A user may not connect to open or shared public-use networks.
    - All wireless networks in use must at a minimum meet the following requirements:

INITIALS
SCORE
End User Acceptable Use Policy

- WPA2 or above security enabled;
- Shared wireless passwords/secrets must be changed every three months.
- Wireless keys must be a minimum of 14 characters in length and meet complex password requirements. (See above)
  - All networks and systems must have proper security controls to ensure malicious users are not connecting to the network with the intent of intercepting SCORE communications or otherwise attacking SCORE systems.
  - The controls must include at a minimum network firewalls and securely configured network equipment to prevent common attack mechanisms.
- Failing to comply or abuse of this policy will result in the loss of access to the SCORE system and could include disciplinary action up to and including criminal prosecution under the provisions of State and Federal law.

USER ACKNOWLEDGEMENT:
I certify that I have reviewed, understand, and agree to the SCORE Acceptable Use Policy. By signing this form, I affirm that I will abide by the SCORE Authorized Use Policy, procedures, and guidelines. I agree to treat all information as sensitive and will not disclose any sensitive information to anyone without the express permission of the Secretary of State. If I have any questions regarding this policy, I will obtain clarification from my supervisor before taking any action.

Name Printed: ___________________________ County: ___________________________
Signature: ___________________________ Date: ___________________________

INITIALS
Statewide Colorado Registration and Election system (SCORE)
County Management Acceptable Use Policy

PURPOSE:
The Score system maintains sensitive information that requires protection. This policy establishes a standard to protect sensitive information contained in the Colorado Department of State SCORE system.

SCOPE:
This policy applies to any person who accesses or uses the SCORE system and any associated equipment that is used to manage, access and or monitor the SCORE system. A representative from each county must sign and agree with this policy. [Reference Colorado Information Security Act (C.R.S. 24-37.5, Part 4) and State of Colorado Cyber Security Program P-CCSP 001, dated December 20, 2006]

INDIVIDUAL RESPONSIBILITIES:
An individual accessing the SCORE system must comply with the following standards and provisions:

• Users are strictly prohibited from sharing passwords or multi-factor authentication devices including grid cards or tokens.

• Users’ complex passwords must:
  o Be at least eight characters in length.
  o Contain three out of the four following items.
     Lower-case letter
     Number
     Upper-case letter
     Symbol
  o Not contain the user’s name or username.
  o Avoid using simple dictionary words. Passwords should be generated from pass phrases that are not written down and are easy for the user to remember.
    ▪ Example: The lazy Dog was under the porch this morning! equates to “TIDwutptm!”

• Users can access, use, or disclose sensitive information only when necessary to perform a job duty. These actions must be expressly authorized.

• Users may not display or provide sensitive information to unauthorized persons. This rule applies to Social Security Numbers contained in document images on workstations, and to other personal and confidential information, such as Date of Birth, Driver License Number, etc.

• Users and their representative employers must ensure proper encryption and handling of sensitive voter information that is downloaded to portable devices such as laptops, PDA’s, memory cards etc.

• SCORE users must ensure proper workstation management and configuration. They must:
  o Only access SCORE on systems that are managed and controlled by the County or State. Users may not utilize a user-owned device to access SCORE.
  o Ensure sensitive information is not displayed on a computer screen in a manner such that unauthorized persons may view the sensitive information.
  o Ensure firewall services including updated versions of antivirus and anti-spyware applications are safeguarding terminals and workstations accessing SCORE.
  o Verify that a complete system anti-virus scan is performed once per month.
  o Ensure workstation maintenance activities are authorized and observed.
  o Ensure the screen is locked to prevent access to SCORE whenever they leave sight of a terminal.
  o Practice safe-surfing habits avoiding potentially malicious Internet sites. Systems utilized to access SCORE sensitive data should not be utilized to browse the Internet whenever possible unless there is a specific allowance specified by the County or State. Counties must have proper mitigating controls in place to prevent malicious web site attacks when business related browsing is permitted.
  o Ensure systems and third party software are fully patched or have proper mitigating controls in place including the following:
    ▪ Operating Systems

SCORE Cyber Security Policy 002
CDOS Rev 1.2
Page 1 of 2
2013-10-29
Statewide Colorado Registration and Election system (SCORE)
County Management Acceptable Use Policy

- Adobe Reader, Flash and Shockwave
- Internet Explorer, Firefox, Chrome and other Web Browsers
- All versions of Java on the machine.
  - Not install or download any software including shareware, freeware, or browser controls unless authorized to do so.
  - Harden all systems to meet industry best practices as specified by County policy. CIS (Center for Internet Security) requirements and other vendors such as Microsoft have published hardening standards for individual operating systems that are updated regularly.
  - Contact the SCORE help desk immediately if system performance becomes erratic, or if it appears the system has been tampered with, or the local virus protection software finds an infection. Degraded system performance or erratic behavior may indicate a Malware infection such as a virus or Trojan.
  - Only connect to county controlled networks with proper network security controls in place. A user may not connect to open or shared public-use networks.
    - All wireless networks in use must at a minimum meet the following requirements.
      - WPA2 or above security enabled.
      - Shared wireless passwords/secrets should be changed every three months.
      - Wireless keys must be a minimum of 14 characters in length and meet complex password requirements. (See above)
    - All networks and systems must have proper security controls to ensure malicious users are not connecting to the network with the intent of intercepting SCORE communications or otherwise attacking SCORE systems.
      - The controls must include at a minimum network firewalls and securely configured network equipment to prevent common attack mechanisms.
    - Failing to comply or intentional abuse of this policy may result in the loss of access to the SCORE system and could include disciplinary action up to and including prosecution under the provisions of State and Federal law.

USER ACKNOWLEDGEMENT:
I certify that I have reviewed, understand, and agree to the SCORE County Management Acceptable Use Policy. By signing this form, I affirm I will abide by the SCORE County Management Acceptable Use Policy. I agree to treat all information as sensitive and will not disclose any information to anyone without the express permission of the Secretary of State or designated election official.

Name Printed: ______________________________________ County: ___________________________
Signature: __________________________________________ Date: ___________________________
RE: Caldara Election Complaint

Dear Mr. Byassee:

The purpose of this letter is to inform you of my decision regarding a complaint that was made in September 2013 against your client, Jon Caldara. Following my office’s three-month investigation into the allegations that Mr. Caldara violated one or more statutes, I have determined that no criminal charges will be filed against him at this time. This decision is being made after a comprehensive review of the currently known facts and after an examination of the applicable state statutes. It is important to note that this decision is being made based on the specific known facts in this matter when compared to the applicable state law. Furthermore, this decision, which follows the above referenced factual and legal review, is being made in accordance with the ethical standards required of prosecutors who administer the prosecutorial function.

As you might be aware on or about September 9-10, 2013 the Office of the Attorney General and two separate District Attorney offices received a citizen complaint. The citizen’s complaint alleged that Mr. Caldara, a long time Boulder County resident and elector, violated one or more Colorado statutes when he participated as a newly registered elector in an El Paso County recall election on Saturday, September 7, 2013, during an early voting period. The day of the actual election was Tuesday, September 10, 2013. Based on the fact that the complaint named Mark Barker, a current Deputy District Attorney in the El Paso County DA’s Office, as being an individual who was supposedly involved with Mr. Caldara and his alleged behavior, the District Attorney for the 4th Judicial District (El Paso and Teller Counties) requested that the Attorney General’s Office investigate the complainant’s allegations.
Regarding the events surrounding this particular election the investigation most clearly demonstrates that Mr. Caldara had multiple goals leading up to and through the election on September 10, 2013. One of Mr. Caldara’s key goals was his intent to make a public statement about one or more issues that he perceived to exist regarding new election related legislation which resulted from the passage of HB 13-1303.

Mr. Caldara’s stated focus on HB 13-1303 and its potential impact on the election process in Colorado was well documented in the public record during the months leading up to the election in El Paso County in September 2013. It appears that Mr. Caldara’s assertion was, that as of May 10, 2013, the Colorado Revised Statutes (most notably § 1-2-217.7, C.R.S.) permitted him, as a registered Colorado voter, to move from one jurisdiction in Colorado to another jurisdiction in this state and then either update his address or register to vote. Additional relevant statutes at issue that must be read in concert include, but are not limited to, §§1-2-101, 1-2-102(1)(f), 1-2-201(3)(a)(V), 1-2-204, 1-2-205 and 1-2-216(4)(a)(I), C.R.S.. As a result, a reading of these various statutes demonstrates an arguable ambiguity within some of the new legislation. This arguable ambiguity was clearly examined in your client’s specific investigation. In Mr. Caldara’s specific case, which is limited by its unique facts and the applicable statutes, a key issue is present. The issue is what does it mean for a resident of Colorado to demonstrate or assert that his or her intention, as a supposed prospective elector, is to make a new county or precinct a permanent residence at the time that he or she is either updating their address or registering to vote?

With Mr. Caldara voicing his opinions about HB 13-1303 and the laws which arose from the bill, it appears that Mr. Caldara then interpreted the new legislation and began to choreograph a series of calculated actions in preparation of the approaching September 10, 2013 recall election in El Paso County. The evidence acquired by the Attorney General’s investigation includes information that prior to Mr. Caldara actually appearing at the El Paso County Citizens Service Center on the morning of Saturday, September 7, 2013, that he had already taken various actions in an attempt to demonstrate his stated intention of becoming a qualified elector in State Senate District 11 (Colorado Springs, El Paso County), including the following:

- On September 6, 2013 Mr. Caldara entered into a residential lease agreement with Deputy District Attorney Mark Barker to rent a bedroom with access to a bathroom and with kitchen privileges at Mr. Barker’s home, which is located at 2045 Broman Ct., Colorado Springs, CO 80906; and
He had changed his home address for his State of Colorado issued Driver’s License from a Boulder County residential address to 2045 Broman Ct., Colorado Springs, CO 80906.

With Mr. Caldara having created a record of his supposed intention to make El Paso County his sole legal place of residence, he went to the El Paso County Clerk and Recorder’s Citizens Service Center September 7, 2013 while accompanied by members of the media. The evidence then shows that Mr. Caldara apparently was given a registration form that he filled out and self-affirmed by signing. It should be noted that Mr. Caldara failed to fully complete this registration form when he did not list the date that he had supposedly moved to 2045 Broman Ct., Colorado Springs, CO 80906. This particular field on the form was a required field and at the top of the form it stated that if the registrant did not provide all of the required information, the application to register to vote would not be complete. Nonetheless Mr. Caldara was in fact registered to vote by the election staff. After Mr. Caldara provided the election staff with a Driver’s License he was given a Paper Ballot (Ballot #01343) for the Senate District 11 Recall Election. The evidence then shows that while Mr. Caldara did submit a ballot on September 7, 2013 he apparently did not cast an actual vote in the particular election. Furthermore, the acquired evidence shows that Mr. Caldara apparently stayed/resided at 2045 Broman Ct., Colorado Springs, CO 80906 on Election Day, September 10, 2013.

On Wednesday, September 11, 2013, the day after the recall election Mr. Caldara left the Broman Ct. address in Colorado Springs and went to his work in Denver. It should be noted that September 11, 2013 was the beginning of the multi-day series of rains that caused the unprecedented flooding that devastated parts of the Front Range, including in Mr. Caldara’s long time hometown of Boulder. In the subsequent weeks after the floods had occurred Mr. Caldara made a public statement that he was reclaiming Boulder County as his home of record. The additional issues created by Mr. Caldara’s post flood statement about Boulder County again being his home is another obstacle in confirming or disproving the veracity of Mr. Caldara’s self-affirmation that, at least on September 7, 2013, his intention was to use the leased residence on Broman Ct. as his sole legal residence. It should be noted that Mr. Caldara then changed his county of residence for voting purposes back to Boulder County in November 2013.

It is imperative to note that the Office of the Attorney General does not condone Mr. Caldara’s choreographed actions that were designed by him to create a record that he used to support his stated intention that at least on September 7, 2013 through September 10, 2013 he was an El Paso County resident and thus was permitted to be a registered elector. Various factors cause me to hesitate when examining the veracity of Mr. Caldara’s intention of being an El Paso County resident on September 7, 2013. In particular I noted Mr. Caldara’s use of a lease agreement with Deputy District Attorney Mark Barker and the circumstances
surrounding this lease as being questionable. While the legitimacy of Caldara/Barker lease arrangement is suspicious, when the available evidence and the applicable law, including arguable ambiguities, are reviewed and compared to the ethical standards for commencing a prosecution, I have determined that a criminal prosecution is not warranted or viable at this time.

Sincerely,

FOR THE ATTORNEY GENERAL

______________________________
Robert S. Shapiro
First Assistant Attorney General

cc: Dan May, Esq.
District Attorney
Office of the District Attorney
105 E. Vermijo Ave.
Colorado Springs, CO 80903