

**Colorado Voter Group**

2867 Tincup Circle  
Boulder, CO 80305

Ms. Melody Mirbaba  
Assistant Attorney General I  
Public Officials Unit  
1525 Sherman Street  
Denver, Colorado 80203

October 2, 2007

RE: September 20, 2007 Colorado Open Records Act ("CORA") request to Colorado Secretary of State Mike Coffman.

Dear Ms. Mirbaba:

In your response letter, dated September 24, 2007, you ask for clarification of five items that we have requested. I hope that these explanations will suffice, but if not, please let us know as soon as possible.

"In particular, please clarify your request numbers A(8), A(9) and A(10). Particularly with regard to request A(10), please clarify whether you are seeking to inspect county security plans." "Additionally, please clarify your request number C(2) with regard to the meaning of "test case library." Also, please clarify your request number C(o) and its sub-parts."

*CORA A(8). Documentation that defines what is meant by "holistic security" and precisely how is it implemented and tested? If it means that the department has conducted an "IBM Application Security Assessment", please provide a copy of the assessment.*

See the reference to "holistic security" on the SOS website. We wish to know what is included.

**Frequently Asked Questions**

[http://www.elections.colorado.gov/WWW/default/Voting%20Systems/FAQs\\_FINAL.pdf](http://www.elections.colorado.gov/WWW/default/Voting%20Systems/FAQs_FINAL.pdf)

Unlike California, Colorado's approach to voting system security is holistic: the electronic voting machines are one part of the election process; the rigorous county security measures in Rule 43 are a key component of that process, as are the acceptance testing, pre-election testing, and post-election audit processes performed at the county level to ensure the integrity of Colorado elections.

We have not found a formal definition of "holistic security" and wonder what the SOS intends to implement and test. When we attended the Public Voting System Demonstrations we asked many questions about elements of the election system that, to our surprise, were not being tested or demonstrated as required. We since have found an assessment instrument developed by IBM and if this is the assessment tool used by the State we wish to inspect the assessment. (See **IBM: A Holistic View of the Security Problem** <http://www.softwaremag.com/L.cfm?Doc=archive/2000oct/IBM.html>, IBM Software Magazine, October 2000 edition)

We are befuddled by the incongruity of the “partial” testing we observed and “holistic” testing. See our request, A(8). Where there are specific requirements on counties, including, “rigorous county security measures in Rule 43... acceptance testing, pre-election testing, and post-election audit processes”, we wish to inspect the documents, files, and information related to the testing that these requirements will be met in future elections, and that these requirements are sufficient to ensure the security of the entire election system.

*CORA A(9). Specification of the threat model.*

Colorado election rules establish requirements for documentation of vulnerabilities and procedures to detect, report, evaluate, respond to and recover from vulnerabilities.

**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.*

Some of us are computer professionals who are also canvass board members and poll watchers. We believe that we have a responsibility to verify the sufficiency of the documentation of threats to the election system, and the responses defined by rule 45.5.2.7.10. We think of this in the context of a threat model, but will accept for inspection any reasonable alternative. For background information regarding the “threat model”, see:

### **Threat Modeling**

<http://msdn2.microsoft.com/en-us/security/Aa570411.aspx>

Threat modeling is composed of three high-level steps: understanding the adversary’s view, characterizing the security of the system, and determining threats.

### **WIKI - Threat model**

[http://en.wikipedia.org/wiki/Threat\\_model](http://en.wikipedia.org/wiki/Threat_model)

Security issues the designer cares about and the description of a set of security aspects

### **Common Criteria – An Introduction**

<http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf>

An evaluation is an assessment of an IT product or system against defined criteria. A CC evaluation is one using the CC as the basis for evaluating the IT security properties. Evaluations against a common standard facilitate comparability of evaluation outcomes.

*CORA A(10). Plan for how the organization will handle security of its trusted networks, over time, against threats from insiders (unintentional mistakes, for example) or outsiders who get past external security controls.*

One threat to the election system comes from insiders, both malicious and unintentional. Outsiders who penetrate the external security controls also represent a significant threat. We wish to inspect the STATE's plan for detecting intrusions and notifying canvass board and other election personnel that such threats have occurred. We wish to inspect how the State will, for example, detect that a Presidential vote has been compromised? (We are unsure if this requires a copy of the county security plans that SOS has approved.) Background on this topic is available at:

**Management and Education of the Risk of Insider Threat (MERIT): Mitigating the Risk of Sabotage to Employers' Information, Systems, or Networks**

<http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tn041.pdf>

**Security Solutions - Data, Devices and the Extended Enterprise**

<http://presentations.inxpo.com/Shows/ZiffDavisEnterprise/VTS/09-26-07/Website/program.htm>

*CORA C(2) Certification test case library including detailed test cases/plans of specific certification tests that are designed to verify and validate each of the following:*

- a) Compliance with Colorado Constitution Article VII section 8 - anonymous ballots.*
- b) Compliance with HAVA requirement regarding voter verification*
- o) ...*

We assume that each element of the election system, defined by Colorado Statutes and Election Rules, is tested for compliance with functional and performance requirements. Professionals usually create collections of tests and test results in what are referred to as test case libraries. This way the tests can be maintained as requirements and results change. We wish to inspect the test case libraries, with specific attention to the requirements identified in the items listed as (a) through (o). If the State does not use the term "test case library", we will accept any reasonable alternative. For background, see:

**Method of and system for managing test case versions**

<http://www.patentstorm.us/patents/6715108-description.html>

*CORA C(o). The following procedures meet functional and performance specifications and are open to poll watchers and canvass board members and the public.*

- i. Logic and accuracy testing*
- ii. Vote interpretation*
- iii. Vote counting*
- iv. Post-election audit*
- v. Canvass process*
- vi. All election procedures and files are verifiable*
- vii. Publication of election files and results*

Colorado Statutes and Election Rules define functional and performance specifications for each of the following seven (7) processes. They also define access requirements for poll watchers and canvass board members, for example:

**CRS 1-7-108.** (3) Each watcher shall have the right to maintain a list of eligible electors who have voted, to witness and verify each step in the conduct of the election from prior to the opening of the polls through the completion of the count and announcement of the results, to challenge ineligible electors, and to assist in the correction of discrepancies.

**CRS 1-10-101.5. Duties of the canvass board.** The canvass board shall reconcile the ballots cast in an election to confirm that the number of ballots counted in that election does not exceed the number of ballots cast in that election. The canvass board also shall certify the abstract of votes cast in any election.

**CRS 1-10.5-107. Canvass board to conduct recount.** (1) Any county clerk and recorder or governing body required to conduct a recount shall arrange to have the recount made by the canvass board who officiated in certifying the official abstract of votes cast. If any member of the canvass board cannot participate in the recount, another person shall be appointed in the manner provided by law for appointment of the members of the original board.

(3) The canvass board may require the production of any documentary evidence regarding any vote cast or counted and may correct the abstract of votes cast in accordance with its findings based on the evidence presented.

To perform their legal duties, poll watchers and canvass board members require access to certain information. This has been a major problem in the past. For example, to date it has been impossible to verify that each individual vote has been correctly interpreted by the electronic system. Also, in certain methods of voting, e.g. vote centers, poll watchers cannot challenge a voter who is voting in the incorrect precinct or who is issued an incorrect ballot style. Also, we cannot determine what criteria are used to determine the integrity of testing results. We wish to inspect the specific tests used to verify that each of the processes meet their functional and performance specifications, and to verify that the requirements of poll watchers and canvassers are met by the election system.

We wish to withdraw our request for inspection of item B2, as we see that the HART outstanding items document has now been published on the SOS website.

We trust that these explanations meet your needs, and look forward to a timely response to our September 20, 2007 Open Records Request.

As you know, the September 20<sup>th</sup> collection of requests has resulted from non-performance by the Department of State in responding to our earlier requests for inspection of records, files and information, as detailed in the attachment to the request. Consequently, we shall need a detailed justification of any costs that might be assessed for staff time.

Also, in the past we have sought records and were told that none exist. It will expedite this matter if you will provide a detailed listing identifying the specific line items where the Secretary of State claims there to be no relevant documents, information or files.

To facilitate communications we have prepared the attached spread sheet which lists each of the items requested. The spread sheet provides space where you can indicate whether the state has full, partial, or no responsive documents/files/information, and whether the state is prepared to produce the documents/files/information for inspection fully, partially, or not at all, and what charge will we incur if we decide to inspect the documents/files/information related to each item. We understand that the State may also charge for the copying of documents/files/information.

Sincerely,



Al Kolwicz  
**Colorado Voter Group**