6 November 2016

Chairman McManus, Vice-Chair Hogan, State Board of Elections Members,

Thank you for the opportunity to address you during the SBE meeting of 28 October 2016. After my presentation, the Deputy Administrator and the Administrator answered questions posed by Chair McManus. I was not given an opportunity to respond to what they said. I am writing to provide my responses—which include technical guidance and suggestions to address the issues of manpower planning and ballot custody—and to make an offer to help conduct a real pilot audit.

As I said at the meeting, because your proposed post-election procedures are not independent of the voting software and do not examine ballots, a finding of no discrepancy has no significance. Maryland's voters are denied the main benefit of paper ballots—confidence in election outcomes. Confidence could be increased greatly if you would augment your plans with a small but robust manual examination of a sample of paper ballots. On behalf of several experts in voting technology and election auditing, I restate the offer I made at the meeting: **we can help you with a real pilot audit; our assistance will be at no expense to the state.**

Technical guidance

A. **Erroneous understanding of what is possible through testing:** Ms. Charlson said that she was confident that the scan data represents the ballots because they had tested the equipment, by having humans compare the scans to the ballots. She also said that she anticipated testing the audit system similarly.

One is tempted to think that the scans consist of a set of images, untouched by any computers, which completely and correctly represent all ballots. Like a set of photographs on film, created by a physical process and not a computerized one. All one needs to do is check that the scanning equipment is well-calibrated and working; as one might check that a film camera is good after looking at a few of the photographs it produces. However, this is not correct. Crucially, while the scans do originate through a physical process, they can only be delivered as ones and zeroes, by software, through the computerized scanner. They are computer data, handled by computer software, and can be deleted, replaced or tampered with.

A reasonably competent attacker would have the software behave differently when tested. Consider, for example, the fact that Volkswagen's 2L Diesel cars were found to use more emission controls when they were being tested than during normal use. On examination, it was found that their software was written so as to detect a test. In our case, software manipulated without vendor knowledge could also present human testers with the scans they expected to see, and then, once it had convinced them that it was performing correctly, it could do something different when used in the election.

B. **Erroneous understanding of the transparency of the proposed post-election procedures:** When the Administrators were asked whether the public would be able to witness the audits, they responded "no," that the audits were software audits and that Clear Ballot would announce the tabulation results after they were obtained and compared with the ES&S counts. There is no difference in transparency between Clear Ballot announcing some results and ES&S announcing some results. Both counting mechanisms are hidden in the software that is running on the respective computers, and there is no evidence being provided to the voter or the candidates that the declared counts match the ballots. Additionally, while ES&S voting systems are federally certified to count votes, Clear Ballot systems are not.

C. **The need for clearly-specified post-election procedures:** I would like to caution the Board to treat both the scan data and the proposed "audits" with care. In particular, if the Board's position is that the scan data does truly represent the ballots, and hence voter intent, and that one can determine whether the election outcome is correct based on this data, then the data should go through all the procedures of a secure chain of custody. When it is data that is being protected, as opposed to ballots, one typically needs to publish digitally signed cryptographic commitments to the data, and check these at every stage. Even so, all one can vouch for is that the other links in the chain are identical to the first one, but not that the first one matches the data collected by the scanning sensor.

As a computer security expert, I have the following questions about the post-election procedures:

1. How does the public know that the scan data represent the ballots?
2. How does the public know that the scan data exported by the scanner is the same data imported by Clear Ballot; that there is no error or tampering?
3. How does the public know that the scan data obtained by Clear Ballot is that processed by Clear Ballot? How are they planning to handle the scan data so that it is not tampered with, with or without their knowledge, while it is in their custody? What is their expertise in computer and information security?
4. What will Clear Ballot do with the scan data? Have they ever performed an audit from scan data in the past? Have they handled audits at the state-level?
5. To determine if the ES&S outcomes are correct, Clear Ballot plans to count votes using the electronic scan data. Is Clear Ballot federally certified to count votes: whether from scan data or directly, from ballots?
6. What information will Clear Ballot provide to the public about the audit procedures as the audits are being performed; and how will they make this information available? How will it demonstrate to the public that the information it is providing is correct? When humans count paper ballots in an audit, the public knows the specifics of the counting process (whether, for example, two people are counting together or one is reading and the other watching etc.), and is typically allowed to observe it. This is a demonstration to the public that the output of the counting process is correct, within well-understood error bounds. Clear Ballot's approach to counting, however, is not known to the public. Even if it were to be described, neither the public nor computer experts would have any means of knowing that the described procedure was the one that ran on the Clear Ballot computer.
7. What happens if the two counts differ in some significant manner? The Board should describe both how it will be involved in adjudicating the difference, and how it will inform the public of this fact.

8. What will be the significance of a finding of no discrepancy between the outcomes, given that the scans themselves may have obscured voter intent from both the primary voting technology and the post-election check?

I urge the Board to treat these issues with the seriousness they deserve. We can help with the above questions as well, but the Administrators have not been forthcoming with details.

On manpower planning and ballot custody

The Administrators' answers to Chair McManus' questions provided some more information about the constraints of the audit.

I understood, from what was said, that the Administrators were concerned about manpower planning and ballot custody issues.

It is possible to carry out a fixed-time-fixed-manpower audit. You would determine, ahead of time, the number of person-hours available for the audit, and the number of physical locations where ballots may be accessed. You can carry out batch-level, or even scanner-level, risk-**measuring** audits, where you examine batches of ballots, get done at a pre-determined time, and announce the risk reduction. That is, you would **not perform a risk-limiting audit** with a pre-specified risk, but, instead, perform the audit you are able to, and declare the quality of the audit once it is done. Perhaps, at that time, it might make sense to concentrate on a particular local race or on a few precincts. **Anything you do that involves independent examination of the paper ballots will provide an infinite improvement in election confidence over what you have now.**

Our offer to help

I can commit to organizing a team of 4-5 experts including myself and other academics, with members chosen for their expertise in election audits and/or voting technology. We can design an audit that meets your constraints, supervise the counting (and comparisons or scanning if you should choose to do those though you don't have to), help you make the random choices (which precincts or batches or ballots to audit) and compute the risk reduction. **Our assistance will be at no expense to the state.**

Maryland can demonstrate the leadership necessary in this election cycle. Its voters deserve as much.

Sincerely,

Poorvi L. Vora

Professor, Computer Science

The George Washington University

Email: poorvi@gwu.edu

Website: https://www.seas.gwu.edu/~poorvi/