27 November 2016

Harvie Branscomb
Coloradans for Voting Integrity

Joe Kiniry
CEO and Chief Scientist
Free & Fair, OR

Mark Lindeman
Adjunct Assistant Professor
Political Science
Columbia University, NY

Neal McBurnett
Consultant on election integrity, CO

Ronald L. Rivest
Institute Professor
Computer Science, MIT, MA

John Sebes
CTO
Open Source Election Technology Institute, CA

Pamela Smith
President, Verified Voting, CA

Philip B. Stark
Professor of Statistics
Associate Dean
Mathematical and Physical Sciences
University of California, Berkeley, CA

Paul Stokes
United Voters of New Mexico

Howard Stanislevic
Founder
E-Voter Education Project
NY, NY

Poorvi L. Vora
Professor, Computer Science
George Washington University, DC

Luther Weeks
CT Voters Count

Comments on:

2016 General Election: Post-Election Tabulation Audit Procedures

Maryland State Board of Elections

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

We are a group of election integrity experts who have collectively been involved in dozens of election audits in dozens of jurisdictions. We have written to you before about your plans for a post-election audit as loosely described in the media. We are writing again to provide more detailed comments on the specific audit procedures described in the online document "2016 General Election: Post-Election Tabulation Audit Overview"[1]. The State Board has invited public comment of those procedures.

In this statement, we focus both on the ways in which the current plan does not meet best practice standards for a post-election audit; and on the ways in which it fails to meet the requirements of the FY17 SBE Budget Amendment,[2] which placed general election audit requirements on the State Board. If the Board fails to adequately meet those requirements, it risks forfeiting a $50,000 administrative appropriation. We argue that the decision to proceed with an audit of scan images—without verifying that those images accurately capture the will of the voters, as represented in the voter-verified paper ballots—circumvents the intent of the FY17 Budget Amendment language and undermines the purpose of carrying out an audit.

---

[1] http://www.elections.state.md.us/voting_system/ballot_audit_plan.html

[2] D38I01.01 Law SB190, enacted under Article III, Section 52(6) of the Maryland Constitution - Chapter 143, detailed in page 22-23 of the report on the budget, 2016 session, attached.

Summary

The FY17 Budget Amendment Chairman's Report requires a tabulation audit of the general election**. The State Board has selected Clear Ballot to conduct this audit, using scan image data captured by the voting system.** The Clear Ballot audit will not involve any hand and eye examination of the actual voter-verified paper ballots at any stage, even if the audit finds significant discrepancies between its own tabulation results and those announced by the voting system. **There can be no audit without a manual examination of the paper ballots.**

We identify the following problems with these procedures:

- A lack of independence: the Clear Ballot audit is not independent because it "audits" the voting system by relying solely on ballot scan data provided by that voting system.
- No valid verification of election outcomes: a finding of "no discrepancy" by the Clear Ballot procedure is not a verification of the election outcome because the procedure cannot "detect and correct any inaccuracies in the machine count" that arise from altered or erroneous scan data.
- Inadequate security procedures for transferring and processing scan images: scan images serve as ballots for the purpose of the audit and should be secured as such.
- Insufficient public comment: public comment was sought only after the audit began.
- No public observation of the audit.

The decision to base the audit solely on electronic scan data is highly inconsistent with best practices, and was made without public comment. We do not consider the justifications provided for the use of only scan data to be valid**.** The scan data that will be treated as official ballots are computer data vulnerable to error, calibration problems and alteration so they may not be an accurate depiction of the voter-verified paper ballots. The suggested pre-audit testing is not sufficient to verify that they are. The Clear Ballot system has **not** been federally certified to tabulate or audit elections. While this may not be an issue in a fully transparent audit, the process currently underway is not transparent.

We are willing to help Maryland design and implement a true, publicly observable audit for this election. By examining only, on average, 112 ballots for the statewide outcomes and 700 for the local federal contests, the audit can provide much greater confidence in the outcome. As we said earlier, our assistance would be at no expense to the state.

Detailed Comments

A: Requirements under the FY17 Budget Amendment to (1) carry out an audit that "can detect and correct any inaccuracies in the machine count due to programming errors, malfunctions, or deliberate tampering that may occur"; and (2) to justify why "hand and eye inspection of actual voter-verified paper ballots is not necessary to reliably determine the intent of the voters", if the audit is not of the paper ballots.

- The Clear Ballot re-tabulation is not independent because it relies solely on ballot scan data provided by the voting system in order to audit the very same voting system.
- The Clear Ballot process cannot verify that the voting system accurately tallied ballots. At best, it can claim that the election tally matches that of the unverified computerized ballot images reported by the voting system software, as administered by local election officials.
- Ballot images are not like true photographs. They are computerized scanner data, and as such are vulnerable to alteration and error—both human error such as the rescanning or dropping of ballots, and scanner calibration error which can result in the sensor not recording marks on the ballots or not sensing certain types of ink.
- Ballot images are not voter-verified and the Clear Ballot audit process will not independently verify them against the voter-verified paper ballots. In fact, the paper ballots might as well not exist. It is proposed that all discrepancies detected in the Clear Ballot audit will be resolved by examining scan data. No discrepancy, however large, will lead to the examination of the paper ballots.
- Pre-audit testing is not sufficient to detect differences between the scans and the ballots. The differences may arise due to alteration, human error, or scanner calibration error. The testing assumes the scanner software will behave, during the election, exactly as it does during the test. A reasonably competent attacker would have the software behave differently when tested[3].
- A procedure that relies only on scans cannot detect missed ballots or those scanned more than once, either through human error or equipment malfunction. It cannot detect whether some ballots were not read correctly due to scanner calibration error. It also cannot detect if ballot scans were altered by malicious software.
- If the state's position is that the scan data stand in for ballots, then the data should go through the procedures of secure custody. However, data

[3] 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 to detect when a test was underway. In our case, software manipulated without vendor knowledge could also provide testers with the scans they expected to see. Then the software could perform differently when used in the election.

security—particularly the transfer of scan data from the voting system to the audit system, and its protection from malware within the audit system—is not addressed at all in the procedures.

- Even perfect agreement between the primary voting system and the audit system would **not** show that the tally was accurate. Both systems derive their conclusions from the same scans (scan data), and neither would detect election outcome errors resulting from differences between the scans and the ballots, or the duplication of some ballots while failing to scan others.

As we have described above, any plausible audit proposal must use a "hand and eye inspection of actual voter-verified paper ballots." Further, actual hand and eye inspection in past audits has detected problems that would have been missed with total reliance on scan data.

For instance, in 2004, in Napa County, CA, a primary election lost 6,000 votes because the scanner was not calibrated to read all types of ink.[4] In 2012, two village council seats in a Florida election were awarded to the wrong candidates because the counting software incorrectly counted votes for one candidate as votes for another. This problem was discovered on a manual audit.[5] Ballot programming errors can happen even when L&A testing is performed. These errors can be detected on manual inspection. In Connecticut, November 2012, a municipality discovered that 151 ballots were double counted because write-in votes were read into the scanner a second time.

B. <u>The choice to use only scan images in Maryland is contrary to best practices.</u> We do not consider the justifications for this decision to be valid.

All audit methods studied in the pilot program earlier this year[6] share the same flaw: They rely only on the computer scans of the ballots, undermining the software independence that audits are designed to achieve. There is one property common to all reliable tabulation audits—independent manual review of the paper ballots. Unfortunately, none of the audit methods studied by Maryland have this property.

The choice to issue an RFI for a system that uses only scan data (no ballots) thus contradicts best practices for election security. In fact, this is likely the reason that there was only one product on the market (Clear Audit by Clear Ballot) capable of accomplishing an audit using scan data from another system. Clear Ballot is performing the audit by simply re-tabulating the scan data; however **this vendor is not federally certified to tabulate ballots**.

---

[4] Kim Zetter, "E-Vote Snafu in California County," *Wired*, 2004. http://archive.wired.com/politics/security/news/2004/03/62721.

[5] Jaikumar Vijayan, "E-voting system awards election to wrong candidates in Florida village," *Computer World*, 2012.

[6] Maryland State Board of Elections, "Post-Election Tabulation Audit Pilot Program Report," October 2016 http://elections.maryland.gov/press_room/documents/Post%20Election%20Tabulation%20Audit%20Pilot%20Program%20Report.pdf.

Claims of efficiency and maximization of technology use cannot be considered sufficient to subvert the goals of the audit; the procedure will miss errors in election outcome caused by differences between scans and ballots. Maryland's General Assembly has clearly stated that the purpose of voter-verified paper records (such as voter-verified paper ballots) is to enable election audits; thus the desire to secure the ballots is not a reason not to perform an audit of the paper ballots. Further, California, Colorado, Connecticut, Minnesota, Montana, New Mexico, New York and Oregon all use paper ballots for their audits, and we are not aware of secure custody issues.

Far more efficient audits are possible for this election. Our calculations show that a carefully-designed audit, examining only, on average, 112 randomly chosen ballots, can provide very good confidence in the contests for President and the Senate. Additionally, by sampling, on average, about 700 of Maryland's 2.5 million ballots, fewer than one-thirtieth of one percent of all ballots, such an audit could greatly improve confidence in the outcome of every federal contest, including contests for House seats. Note that this audit would not use any of the scan data and not scan any ballots. Further, it does not require that ballots be stored in the order in which they were scanned.

C. Requirement for public comment and public observation of audit

The proposed procedures were carried out without public comment and are not publicly observable.

- The FY17 SBE Budget Amendment Chairmen's Report requires that the public have an opportunity to comment on audit procedures as they are developed. The SBE, however, only called for public comment long after the pilot audit for the primary election had been completed; and only after the audit for the general election had begun. Moreover, the call for public comment had insufficient notice to the public and was not done through the normal process of the Maryland Registrar. The comments, now submitted, are focused on an audit procedure that has been completed. A major departure from best audit practices was made without any opportunity for public comment.

- The FY17 Budget Amendment requires that the audit procedures be publicly observable; but the proposed software audit is inherently unobservable because it occurs on Clear Ballot software without public documentation of the algorithms to interpret ballots, using private computers, in an unannounced location. The public was not provided any information while the audit process was ongoing, defeating the very purpose of transparency. For example, as of writing these comments, Clear Ballot's "Preliminary Statement of Votes Cast", which the Overview states was to be provided before November 16, ηas not been made available to the public. Has it been submitted to the State? Will it be provided to the public at the end of the process or will the public only obtain the final reports? The Overview states that Clear Ballot will provide this information before it obtains precinct-level results so that the audit is "blind," because Clear Ballot will not know the

correct result before submitting this report. None of the data is provided to the public—so how does the public know that the preliminary statement was not modified to make it consistent with the precinct-level count?

D. Requirement to report the calculated risk

With Maryland's current procedures, in the event that the ballots and scan data do not match, the risk that a change in election outcome is undetected can be very large. In the event that such a mismatch were to result from malicious intent, the risk is close to 100%. The State is required to report this under the FY17 Budget Amendment.

It is not too late to audit the election. We can help the Board conduct a proper audit by committing to a team of 4-5 experts, including academics, chosen for their expertise in election audits and/or voting technology. We can design an audit that meets your constraints, supervise the procedure (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. We can also help you design an audit procedure that can be used in the future. **Our assistance will be at no expense to the state**.

In passing HB18 of 2007, and authorizing the switch to a voter-verified paper ballot/optical scan voting system, the Maryland General Assembly anticipated that voting on paper ballots would lead to a true audit of those ballots[7]. This is an opportunity for Maryland to demonstrate the national leadership to which it aspires. It also provides voters, candidates, and political parties the confidence in the election outcome which they deserve—and which the Budget Amendment requires.

[7] Md. Election Law Code Ann. § 9-102. (h)(2) *The regulations shall specify the procedures necessary to assure that the standards of this title are maintained, including: (xi) assuring ballot accountability in systems using a document ballot; (xii) the actions required to tabulate votes; and (xiii) postelection review and audit of the system's output*.

Biographies

Harvie Branscomb is an electrical engineer, election technologist and election quality advocate. He has conducted numerous statutory election audits in Colorado. He has served as a credentialed watcher of elections across the state including several pilots of innovative tabulation and audit techniques. He served on several Colorado Secretary of State appointed advisory committees including one leading to the choice of the Uniform Voting System. Branscomb is a regular participant in public testimony on election rules and statutes. He is a board member of Coloradans For Voting Integrity. He is also CEO of StandbySoft LLC. Branscomb an A.B. Magna Cum Laude from Cornell University and S.M. (Master of Science) in Electrical Engineering and Computer Science from M.I.T.

harvie@electionquality.com

http://electionquality.com/

Joseph Kiniry, is the CEO and Chief Scientist of Free & Fair, a public benefit corporation whose goal is to foster trustworthy elections through trustworthy technology worldwide. He is also a Principal Investigator at Galois, where he leads programs in high assurance cryptography, rigorous engineering, and formal methods-based audits. His clients include federal agencies and large public corporations. Previously he was a Full Professor at the Technical University of Denmark (DTU). There, he was the Head of DTU's Software Engineering section. He also held a guest appointment at the IT University of Copenhagen. Kiniry has extensive experience in formal methods, high-assurance software engineering, foundations of computer science and mathematics, and information security. Specific areas that he has worked in include software verification foundations and tools, digital election systems and democracies, smart-cards, smart-phones, critical systems for nation states, and CAD systems for asynchronous hardware. He has fifteen years' experience in the design, development, support, and auditing of supervised and internet/remote electronic voting systems while he was a professor at various universities in Europe. He co-led the DemTech research group at the IT University of Copenhagen and has served as an adviser to the Dutch, Irish, Danish, and U.S. governments in matters relating to electronic voting. Kiniry has a Ph.D. from California Institute of Technology (Caltech).

kiniry@galois.com

https://galois.com/team/joe-kiniry/

Mark Lindeman is a political scientist whose research includes public opinion, political behavior, and election verification issues. His work with post-election vote tabulation audits includes writing several co-authored methods papers; serving as executive editor of the 2012 white paper "Risk-Limiting Audits: Why and How" on behalf of a multidisciplinary working group; and advising officials

and advocates in several states about audit implementation. He is co-author of *Public Opinion* (third edition: Perseus Westview, 2015). Lindeman has a Phd from Columbia University.

MTL4@columbia.edu

Neal McBurnett is an independent consultant in election integrity and security. He has worked for Bell Labs, Internet2 and Databricks. He has worked to improve election integrity since 2002 by pioneering post-election audits, working with election administrators, legislators and secretaries of state. He did the first risk-limiting audit in Colorado, and collaborated on Colorado's Risk Limiting Audit project and ballot-level risk-limiting audits that reached new levels of efficiency and scale. He also audited the innovative Scantegrity end-to-end-verifiable election in Takoma Park MD in 2011, and is a member of the STAR-Vote design team.

McBurnett has also worked on data format standards for elections via the IEEE and the US Election Assistance Commission (EAC), and is active with the Election Verification Network. McBurnett has a BS in computer science from Brown University and an MS in computer science from University of California, Berkeley.

nealmcb@gmail.com

http://bcn.boulder.co.us/~neal/elections/

Ronald L. Rivest is the Institute Professor of Computer Science in MIT's Dept. of Electrical Engineering and Computer Science. He is a member of MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL), a member of the lab's Theory of Computation Group and is a leader of its Cryptography and Information Security Group. He is a founder of RSA Data Security and an inventor of the RSA public-key cryptosystem, and a co-founder of Verisign and of Peppercoin. Professor Rivest has research interests in cryptography, computer and network security, voting systems, and algorithms. He is a member of the National Academy of Engineering, the National Academy of Sciences, and is a Fellow of the Association for Computing Machinery, the International Association for Cryptographic Research, and the American Academy of Arts and Sciences. He is also on the EPIC Advisory Board.

Together with Adi Shamir and Len Adleman, Rivest was awarded the 2000 IEEE Koji Kobayashi Computers and Communications Award and the Secure Computing Lifetime Achievement Award. He also received, together with Shamir and Adleman, the 2002 ACM Turing Award and the 2009 NEC C&C Prize. He received an honorary degree from the University of Rome. He is a Fellow of the World Technology Network and a Finalist for the 2002 World Technology Award for Communications Technology. In 2005, he received the MITX Lifetime Achievement Award; in 2007, he received both the Computers, Freedom and Privacy Conference "Distinguished Innovator" award and the Marconi Prize. In 2008, he received an honorary doctorate from the Louvain School of

Engineering at the Universite Catholique de Louvain (UCL). In 2010, he was awarded MIT's Kilian Faculty Achievement Award. He has extensive experience in cryptographic design and cryptanalysis, and served as a Director of the International Association for Cryptologic Research, the organizing body for the Eurocrypt and Crypto conferences, and as a Director of the Financial Cryptography Association.

rivest@mit.edu

https://people.csail.mit.edu/rivest/

E. John Sebes is one of the two original co-founders and Chief Technology Officer ("CTO") for the U.S. based non-profit public benefit corporation, the Open Source Election Technology Institute ("OSET"). He leads all aspects of technology strategy, vision, architecture, engineering and development for the TrustTheVote Project – the flagship effort of the Institute.

Sebes has been a software developer, technical consultant, and CTO, working in several areas - network infrastructure, application frameworks, embedded systems, critical infrastructure, datacenter operations - with strong common themes of risk management, security, privacy, and reliability. Innovation and tech transfer have been another consistent theme, in settings as varied as government-funded R&D, venture-backed start-ups, professional services, academia, and non-profits.

Sebes is a co-author of 12 patents and 20+ publications

Pamela Smith is President of Verified Voting. She provides information and public testimony on verified voting issues at federal and state levels throughout the US, including to the US House of Representatives Committee on House Administration. She oversees an extensive information resource on election equipment and the regulations governing its use at the federal level and across the 50 states. Ms. Smith is co-editor of the "Principles and Best Practices for Post-Election Audits," co-author of "Counting Votes 2012: a State by State Look at Election Preparedness" and a contributing author for *Confirming Elections: Creating Confidence and Integrity through Election Auditing*.

pam@verifiedvoting.org

https://www.verifiedvoting.org/

Howard Stanislevic has been a computer network engineer for over 25 years in NYC working in various industries including telecommunications, airlines and advertising. He has worked on such diverse projects as domestic satellite digital audio transmission systems and the Washington-Moscow "Hotline." In his spare time, he has worked with the Internet Engineering Task Force and has contributed to several Requests for Comments (RFCs—formalized peer-reviewed memoranda addressing and defining Internet standards). He has been studying the e-vote-counting problem since 2004, and has become a full-time advocate

for verified elections (not just "verifiable" ones). He co-authored the first risk-based statistical audit law in the nation, NJ C.19:61-9 (PL 2007 Ch. 349) and papers on election auditing, voting system reliability and standards published by The American Statistical Association, Verified Voting and VoteTrustUSA. He has contributed to NY State's Voting System Standards and two drafts of NY's Election Auditing and Recanvass regulations.

Philip B. Stark is Professor of Statistics, Associate Dean, Division of Mathematical and Physical Sciences, and Director of the Statistical Computing Facility at the University of California, Berkeley. Stark is on the Board of Advisors of the US Election Assistance Commission. He developed the notion of "risk-limiting audits", which are now required by the state of Colorado (C.R.S. 1-7-515) and this work has led to audit-related legislation in California: California AB2023, SB360, AB44. He served on California Secretary of State Bowen's Post Election Audit Standards Working Group. Stark has published more than one hundred fifty articles and books, served on the editorial board of several scientific journals, and lectured at universities and professional societies in more than twenty-five countries. He has consulted for the U.S. Department of Justice, the Federal Trade Commission, the U.S. Department of Agriculture, the U.S. Census Bureau, the U.S. Department of Housing and Urban Development, the U.S. Department of Veterans Affairs, the California Attorney General, the California Highway Patrol, and the Illinois State Attorney. He has testified to the U.S. House of Representatives Subcommittee on the Census; the State of California Senate Committee on Elections, Reapportionment and Constitutional Amendments; the State of California Assembly Committee on Elections and Redistricting; and the State of California Senate Committee on Natural Resources. Stark received the University of California Chancellor's Award for Public Service for Research in the Public Interest and the Leamer-Rosenthal Prize for Transparency in Social Science.

stark@stat.berkeley.edu

https://www.stat.berkeley.edu/~stark/

Paul Stokes spent most of his career at Sandia National Laboratories conducting research, development and analysis of technologies for arms control compliance verification and intelligence, and later at the International Atomic Energy Agency in Vienna, Austria, conducting nuclear inspections in Iraq, and at the Comprehensive Nuclear Test Ban Treaty Organization, also in Vienna, developing on-site inspection techniques.

Stokes has been engaged in election integrity activities since the 2004 election, when he worked with national organizations to pursue a recount, followed by support for legal action to investigate the accuracy of voting machines. Since that time, as coordinator for United Voters of New Mexico, Stokes has continued to work with state election officials and the Legislature to bring the uniform use of paper ballots throughout the state, and post-election audits to verify with high confidence the accuracy of voting machines. He continues to work on

Election Integrity by advocating methods to improve voter access to the polls. Stokes has B.S. and M.S. degrees in Electrical Engineering from North Dakota State University and the University of New Mexico respectively.

stokescorrales@mac.com

Poorvi L. Vora is Professor of Computer Science at The George Washington University. Her research focus has been on end-to-end independently verifiable (E2E) voting systems which enable voters and observers to audit election outcomes without requiring them to rely on the trustworthiness of election technology or unobserved election processes. Vora was a member of the team that deployed polling-place, paper-ballot-based, E2E voting system Scantegrity II in the Takoma Park elections of 2009 and 2011, and of the team that developed remote voting E2E system Remotegrity and accessible voting variant Audiotegrity, used in 2011. She has worked with the National Institute of Standards and Technology (NIST) on definitions of desired properties of E2E systems, and on information-theoretic models and measures of voting system security properties. Her research is funded by the National Science Foundation and the Maryland Procurement Office. Vora has a Ph.D from North Carolina State University.

poorvi@gwu.edu

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

Luther Weeks is Executive Director of CT Voters Count. He is a retired software engineer, and a computer scientist who has been active for several years in voting integrity issues and citizen-lobbying the Connecticut Legislature and the U.S. Congress.

Weeks' efforts in Connecticut contributed to the passage of the paper record law in 2005 and the selection of optical-scan over DRE (touch screen) voting equipment in 2006. In 2007, he organized a coalition of citizens to observe Connecticut's post-election audits resulting in public legislative hearings across the state. He is also Executive Director of the Connecticut Citizen Election Audit and a Director of TrueVoteCT.

Spanning thirty-five years, Weeks led the initial implementations of database, personal computer, and artificial intelligence technologies for The Travelers, where he also led the evaluation and acquisition of commercial software. In the 1990's, for nine years, he was a field engineer and product manager for two data communications software start-ups. Weeks has a B.S. in Mathematics with distinction from Clarkson University and an M.S. Computer Science from Rensselaer Polytechnic Institute. He is Master Fellow of the Life (insurance) Management Institute.

Luther@CTVotersCount.org

http://www.ctelectionaudit.org/