Maryland Legislature:
House Ways and Means Committee
Senate Education, Health and Environmental Affairs Committee

Joint Hearing on Election Cybersecurity

Expert Testimony by
Poorvi L. Vora
Professor of Computer Science, The George Washington University

6 September 2017

Chair Kaiser, Chair Conway, members of the House Ways and Means Committee and the Senate Education, Health and Environmental Affairs Committee: thank you for the invitation to speak at this hearing. I am a Professor of Computer Science at The George Washington University. My research of the last fifteen years has been in the general area of computer security and privacy, with a special emphasis on the integrity of electronic voting systems[1].

My testimony today represents what I have learned from my own research and that of hundreds of others over about four decades[2,3,4,5,6,7,8,9,10]. The literature in this field is

[1] My qualifications and complete CV, as well as more details about my work, may be found on my website: http://www.seas.gwu.edu/~poorvi/

[2] P.A. Karger and R.R. Schell, "Multics Security Evaluation: Vulnerability Analysis", *ESD-TR-74-193*, Vol. II, June 1974, HQ Electronic Systems Division: Hanscom AFB, MA. http://csrc.nist.gov/publications/history/karg74.pdf

[3] Roy Saltman, "Accuracy, Integrity, and Security in Computerized Vote-Tallying", *Special Publication (NIST SP) - 500-158*, National Institute of Standards and Technology, 1 August 1988. https://www.nist.gov/publications/accuracy-integrity-and-security-computerized-vote-tallying

[4] Rebecca Mercuri, "Voting-Machine Risks," Inside Risks, *Communications of the Association for Computing Machinery*, Volume 35, No. 11, November, 1992. http://www.notablesoftware.com/Papers/votemachrisk.pdf

[5] Rebecca Mercuri, "Electronic Vote Tabulation Checks & Balances," Ph.D. dissertation, University of Pennsylvania, Philadelphia, October 2000. http://www.notablesoftware.com/Papers/mercuri-thesis.pdf

[6] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, "Analysis of an Electronic Voting System," *Johns Hopkins Information Security Institute Technical Report TR-2003-19*, July 23, 2003. http://avirubin.com/vote/ Also published in *Proceedings of the IEEE Symposium on Security and Privacy*, 2004. DOI: 10.1109/SECPRI.2004.1301313 http://ieeexplore.ieee.org/document/1301313/

[7] Ronald L. Rivest and John P. Wack. "On the notion of `software independence' in voting systems", 2006. https://people.csail.mit.edu/rivest/RivestWack-OnTheNotionOfSoftwareIndependenceInVotingSystems.pdf

unambiguous and non-partisan: computerized election systems—whether connected to the internet or not—provide opportunities for the intentional alteration of election outcomes. They are also vulnerable to human and machine error.

The two recommendations from the scientific community are also unambiguous and non-partisan[11]: first: the internet-facing parts of our election systems need to be hardened to protect against attacks and to enable the detection of as many attacks as possible. For Maryland, a first step would be to appoint a permanent team of policy makers and experts to guide and supervise on election cybersecurity issues. Election administration today requires the operation of a large complicated computer infrastructure targeted by competent, motivated, foreign adversaries. Technical expertise in oversight is needed on an ongoing basis to ensure that cybersecurity concerns are addressed in decisions about election procedures and technology and do not present larger problems later[12].

Second, the scientific community warns that we should not expect that all errors or attacks on our vote tallying systems will leave an electronic trail. Having had the foresight to act on this issue a decade ago, Maryland generates and stores durable paper ballots, which provide voter-verified evidence of voter intent. This is not sufficient, though. Voters need to know that the election outcome was correctly computed from the voted ballots. Hence an independent, public, risk-limiting audit[13] of the election outcome, using the paper ballots as the starting

Prepared for the TGDC, and posted by NIST at the given url. (2006-07-28). Also published as: Ronald L. Rivest. "On the notion of `software independence' in voting systems." *Philosophical Transactions of The Royal Society A* 366,1881 (2008) pp. 3759--3767.

[8] "Top to Bottom Review", State of California, 2007. http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/

[9] Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine" *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07)*, Boston, MA, August 2007. https://jhalderm.com/pub/papers/ts-evt07.pdf

[10] "EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing", Final report, December 2007. http://www.patrickmcdaniel.org/pubs/everest.pdf

[11] See, for example, a letter to the US Congress signed by about a hundred international experts; pg. 8 of Prof. Alex Halderman's recent testimony to the Senate Select Committee on Intelligence on the topic of Russian Interference in the 2016 election https://jhalderm.com/pub/misc/ssci-voting-testimony17.pdf

[12] These include decisions about the choice of voting systems and audits, the security of online voter registration, ballot delivery and ballot marking tools, wireless technology, network protection, and in-house software development vs the use of commercially available software.

[13] See J. Bretschneider, S. Flaherty, S. Goodman, M. Halvorson, R. Johnston, M. Lindeman, R.L. Rivest, P. Smith, and P.B. Stark, "Risk-Limiting Post-Election Audits: Why and How", 2012 http://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf Risk Limiting Audits are endorsed by the American Statistical Association, see http://www.amstat.org/policy/pdfs/StarkEtAlLetterOfSupport.pdf Post-election audits of both the election outcome and the election technology are recommended by the Presidential Commission on Election Administration, see: "The American Voting Experience: Report and Recommendations of the Presidential Commission on Election Administration", January 2014, pg 66, https://law.stanford.edu/wp-content/uploads/sites/default/files/publication/466754/doc/slspublic/Amer%20Voting%20Exper-

point, should be performed after every election. An election should be certified only after it passes the audit.

Maryland does not yet perform such an audit.

Before I talk some more about how Maryland may approach such audits, I would like to speak briefly to the context today, and how it affects Maryland. We have heard that the voter database breaches in the news have nothing to do with vote tallies. This is not completely true. While they do not directly touch voting machines, voter database breaches can enable access to voter credentials, which is a first step in casting fraudulent absentee ballots. This is not an abstract threat—it has been reported that actors from Russian military intelligence were trying to fake absentee voting services last year[14].

Maryland is particularly vulnerable because of no-excuse electronic ballot delivery for all and no signature comparison once the ballot is received[15]; additionally, we have learned through the Legislative Office's Audit Report that voter data was not sufficiently protected by the state[16]. It has been reported that Maryland did not find evidence of entry into its database[17]. However, we should not presume to know with certainty that the database was not breached, or that it is secure going forward; competent attackers can conceal signs of a breach, and classified federal information regarding serious breaches would not be revealed without security clearance.

final%20draft%2001-04-14-1.pdf and "Report on Election Auditing" by the Election Audits Task Force of the League of Women Voters of the United States, January 2009, http://lwv.org/files/Report_ElectionAudits.pdf

[14] A top secret NSA report released by The Intercept describes a spear phishing attack attributed to the Russian military intelligence, GRU. It reports that GRU obtained the email credentials of at least one employee of pollbook manufacturer VR Systems, and used these to contact 122 email addresses of local government employees or officials, attempting to infect their computers with malicious software embedded in Microsoft Word documents. See "NSA Report on Russia Spear Phishing" https://assets.documentcloud.org/documents/3766950/NSA-Report-on-Russia-Spearphishing.pdf

While there is no evidence that these efforts were successful, the state of North Carolina experienced voter registration problems very similar to those that could be caused by the manipulation of data on their pollbooks, which are provided by VR Systems. See Pam Fessler, "Russian Cyberattack Targeted Elections Vendor Tied To Voting Day Disruptions", NPR, 10 August, 2017. http://www.npr.org/2017/08/10/542634370/russian-cyberattack-targeted-elections-vendor-tied-to-voting-day-disruptions

The NSA report also describes how the same actors appeared to be trying to fake absentee voting services.

[15] The National Institute of Standards and Technology recommends that signatures form the primary authentication mechanism for returned absentee ballots, see "Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters", NIST IR 7711, Sept 2011, https://www.nist.gov/document-9678.

[16] There have been other issues with voter information and Maryland databases. See, for example, minutes of the Montgomery County Board of Elections Meetings, 16 May 2016 (pg. 10) and 18 July 2016 (pg. 6) for the unexplained deletion of "credits" for 1600 absentee ballots without a log entry for the deletion.

[17] Michael Dresser, "Maryland elections board says it detected 'suspicious activity' last fall", The Baltimore Sun, 14 June 2017. http://www.baltimoresun.com/news/maryland/politics/bs-md-voting-suspicious-20170614-story.html

We do not know how successful foreign actors were in their efforts to breach election security in the US, or what their final technical goals were. But we are certain they tried. There is virtually complete consensus in the scientific community that the vulnerable state of our technology poses a serious threat to our elections and, consequently, our democracy.

Audit Possibilities for Maryland

I will now turn to how Maryland can tell that its election outcomes, as determined by its voting system, are correct and represent voter intent.

2016 retabulation procedure

Last year, the state contracted a third party vendor to retabulate the election. That is, the third party vendor got ballot images provided by the voting system and counted them using its own software. This procedure identified some problems that affected vote tallies, though these problems did not influence the election outcomes[18].

The procedure is not a satisfactory audit of the election outcome. First, though it is a third-party procedure, it is not independent. It relies on digital scans of the ballots provided by the very voting system being audited, and does not access the voter-verified paper ballots at all.

Second, ballot scans are computer-generated and computer-manipulated data, not verified by voters. Like all computer data, they are vulnerable to error, alteration, deletion, and fabrication. In the event of a mismatch between the ballot images and the ballots—whether due to machine or human error or malicious intent—this procedure will not detect any resulting errors in the election outcome. Beginning from the same flawed data—which does not constitute voter-verified evidence—it will make the same errors.

In particular, this procedure would not detect a competent effort to manipulate the election outcome by manipulating ballot image data. A finding of "no discrepancy" from this procedure is hence not meaningful. Its use as an election audit defeats the very purpose of storing durable voter-verified evidence in the form of paper ballots.

Would you accept a very efficient home inspection that relied solely on photographs of the house provided by the builder? Perhaps the inspection of photos would reveal useful information, such as a broken window. Does that mean that physical examination of the roof, the electrical systems and plumbing is not necessary?

[18] For example, the third party found that ballot folds were being interpreted as marks, and hence over-votes, by the voting system.

There are other problems with the third party tabulation. It is carried out by software, inside a computer, and is not transparent to the public. Last year, it was carried out on vendor premises in Boston, Massachusetts.

Finally, for two groups of voters, the procedure did not even access ballot scans of voter-verified evidence[19]. For absentee voters receiving ballots online, it relied on scans of manual reproductions made by election workers and never seen by voters. For votes cast using the Express Vote ballot marking system, used by voters with disabilities, it relied on unverified barcode encodings of the votes.

Risk Limiting Audits

I wrote several letters to the State Board of Elections, many with other experts, communicating our concerns[20]. We recommended other types of audits[21] that would access the voter-verified ballots and provide robust evidence of election outcome correctness and *offered our help in carrying out the audits at no cost to the state*. We recommended the use of ballot polling audits[22], ballot comparison audits[23] or batch comparison audits. In all these audits, some ballots or ballot boxes are chosen at random and individual ballots are manually examined to determine voter intent. The number of ballots that need to be handled depends on the type of audit, its quality and the margin.

[19] Absentee votes were manually reproduced by election workers, and the ballots scans used were of the newly-made ballots, not of the mailed-in voter-verified ones. Voters with disabilities use the Express Vote machine to print their completed ballots. These ballots list the winners and an associated barcode, and do not have marked ovals. The procedure ignored the listed winners on the ballot and interpreted the barcodes, which were not voter-verified.

[20] Some Observations re: Maryland's Election Procedures, 2016. http://www2.seas.gwu.edu/~poorvi/MarylandAudits/

[21] Mark Lindeman and P.B. Stark, "A Gentle Introduction to Risk-Limiting Audits", *IEEE Security & Privacy*, 10, 42–49. https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf

[22] In a ballot polling audit, ballots are drawn at random and used to estimate the election outcome, in much the same way that a poll is used to estimate who the winners would be. The number of ballots that need to be drawn depends on the margin, and the desired probability of detecting an incorrect outcome. Note that this audit does not attempt to determine if the vote count is correct, only whether the outcome is. As an example, from preliminary contest counts declared by the state in the 2016 election, we observed that Maryland could have achieved at least a 95% probability of detecting an incorrect outcome in both the statewide contests by manually inspecting about 112 randomly chosen ballots from the entire state.

Because Maryland's margins were large last year, by manually inspecting some more ballots—about 700 of 2.5 million, fewer than one-thirtieth of one percent—Maryland could have achieved at least a 95% probability of detecting an incorrect outcome in each federal contest, including contests for seats in the US Congress.

[23] In a ballot comparison audit, individual ballots are compared to their electronic interpretations, or cast vote records (CVRs). For a comparison at this fine-grained level, ballots would need to be rescanned by the DS 8500 central scanner, which can imprint numbers on the ballots to enable comparisons with the numbered CVRs.

The quality of an audit is quantified by its risk limit, which is the maximum probability that the audit will fail to recognize an incorrect election outcome. A lower risk limit implies a better audit, which is less likely to miss an incorrect outcome.

Risk Measuring Audits

We understood that the Administrators were concerned about manpower planning for risk-limiting audits in the event of small margins, when the number of audited ballots is expected to be large. For this reason, we also suggested the possibility of carrying out a fixed-resource audit. You would not perform a risk-limiting audit with a pre-specified risk limit, but, instead, commit to performing an audit that examined a certain number of ballots or ballot boxes, perform it, and calculate and declare its quality (risk) once it is done[24].

The best specific type of audit for a given risk, margin and contest size will depend on an assessment of the cost (personnel hours, effort, financial cost) of each audit and would need to be determined in collaboration with election officials and the state administration. An Appendix to my written testimony contains some audit comparisons. I would be happy to discuss these comparisons further and to help you determine which audit to perform.

My rough audit comparisons, based on timing measurements reported in the SBE's pilot audit report from 2016, indicate that audits of the federal and statewide contests would not take as long as some might fear. This is consistent with the pilot audit report itself, which found that it took much less time to carry out the ballot comparison and batch comparison audits than did the *preparation* for the Clear Ballot audit.

In Conclusion

- Maryland should appoint an advisory body on election cybersecurity.
- Maryland should carry out **independent** and **public** post-election tabulation audits that are **based off voter-verified evidence**[25].
- Audits of contests for statewide or federal office should be **risk-limiting**[26], with a risk limit of 5% (10% if you do not have the resources for a 5% audit).

[24] 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 could then 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.

[25] This includes the original voted paper ballots for early, in person and absentee voters, and the vote itself (not the bar code) for Express Vote ballots generated for voters with disabilities.

[26] If the 5% risk limit presents too large a burden on local contests, particularly those with small margins, these contests may be audited to pre-determined constraints, such as minimum number of ballots examined. The resulting measured risk should be announced.

- Counties and the SBE are not prevented from audits with lower risk limits, or from auditing other contests. In fact, it is highly recommended that all contests be audited.

In the event that you decide to propose legislation on this issue, I, and my colleagues who offered to help last year, would be happy to help you draft the legislation or review it and provide comments. As was true last year, this offer is at no cost to the state.

Thank you for your time.

Appendix A: Audit Comparisons

Types of audits

- **Ballot polling audits:** tally randomly chosen ballots from the entire election, like a poll.

- **Batch comparison audits**: hand count randomly-chosen ballot boxes and check system tally of those boxes

- **Ballot comparison audits:** compare the randomly-chosen physical ballot to the system's electronic cast vote record

Possible Audit Approaches

Method	Pros	Cons	Cost
Ballot Polling Audit 2016 Presidential margin requires 100 ballots polled on average	Works for any voting system	Inefficient for narrow margins No quality improvement feedback	Personnel time only
Ballot Box Tally Comparison. Number audited depends on margin (as in New Mexico)	Works for any voting system	More ballots handled but fewer random choices; fewer ballot boxes	Personnel time only
Rescanning with DS850 or 3rd party + Ballot Comparison Audit	Fewer ballots examined Helpful in identifying source of problems	Needs rescanning	Personnel time only
3rd party retabulation + any above Audit	Quality improvement feedback	Expense	$275K + personnel time
3rd party retabulation only	**NOT AN OPTION**		