Philip B. Stark • Dept. of Statistics • University of California • Berkeley, CA 94720-3860

Mr. Alex Padilla
Secretary of State
1500 11th Street
Sacramento, CA 95814

January 20, 2020

Comments on VSAP security defects and certification

Dear Secretary of State Padilla:

I am Professor of Statistics and Associate Dean of Mathematical and Physical Sciences at the University of California, Berkeley. I serve on the Board of Advisors of the U.S. Election Assistance Commission (EAC). I served on former Secretary of State Debra Bowen's Post Election Audit Standards Working Group. I helped draft AB44, SB360, AB2123, and AB2125, and I have served on your working group to draft regulations to implement AB2125.

I write as an individual, not as a representative of my employer, the US EAC, or any other entity. The opinions expressed below are my own.

The VSAP system has a number of serious security and usability flaws. I do not think it should be certified until and unless all critical issues have been fixed, verified to have been fixed by additional testing, and the remediations and testing results have been published.

While there are serious security problems with several parts of the VSAP system, below I focus primarily on the ballot-marking device (BMD).

The intrinsic security flaws of BMDs have only recently been understood and documented. Like all electronic devices, BMDs can be misconfigured and hacked. Post-election audits, including risk-limiting audits, cannot detect or correct problems that caused BMDs to print incorrect votes on the paper record. It has been tacitly assumed that voters will check the printout themselves and report problems. However, empiri-

cal research over the last two years shows that voters themselves rarely check the paper record—even when prompted to do so verbally and in writing—and rarely detect errors introduced by BMDs. Moreover, research on the underlying security model for BMDs (which relies on voters to detect malfunctions and hacking) shows that even if voters could be relied upon to catch and report the vast majority of errors, that would not suffice to make elections conducted largely on BMDs trustworthy.

Risk-limiting audits of BMDs do not test whether the BMDs functioned correctly: there is no testing procedure that can in practice. See Stark (2019b).

1. The system requires *all* in-person voters to use the BMD. This undermines the trustworthiness of the paper trail, as shown by DeMillo et al. (2018), Appel et al. (2019), Stark (2019ab), and Bernhard et al. (2020), effectively eliminating the security advantage of a paper record of the votes. Until there is a demonstrably better option, voting systems should use hand-marked paper ballots primarily, reserving BMDs for voters who require accommodations to vote independently.
2. The design of the VSAP BMD is defective from a security perspective: the ballot passes under the printhead after the voter last sees the paper. This enables the "opportunity to mark" flaw.
   https://securiosa.com/posts/how_the_expressvote_xl_could_alter_ballots.html
   The use of a cam to lift the printhead while the ballot is cast is not adequate protection, because that cam is itself controlled by software. The paper path for casting the ballot should not include the printhead. The ballot box should be physically separate from the BMD, or at least not in the same path as the printer.
3. While I have not been able to verify this from the documentation, the BMD appears to have an "autocast" function, also known as "permission to cheat," whereby a voter can tell the machine to print and cast the paper before the selections have been printed.
   https://freedom-to-tinker.com/2018/09/14/serious-design-flaw-in-ess-expressvote-touchscreen-permission-to-cheat/ If that is true, the feature should be eliminated.
4. Applying RLA procedures to BMD output does not result in a true RLA, because the paper trail is not trustworthy: the BMD can print something other than what the voter saw on the screen or heard through the audio interface. As a result, there is no way to ensure that incorrect outcomes are (with high probability) corrected by the audit.
5. Many administration functions require root access. This is a serious security flaw. The system should be re-designed with appropriate roles and permissions

so that routine functions involved in election configuration and vote tabulation do not require root access. Root access should be reserved for highly trusted individuals who genuinely need it.

6. I understand that the "more" button has been improved, but I strongly suspect that the user interface will lead some voters to overlook some candidates. A possibly better solution would be to require voters to view all pages of a contest before allowing them to make a selection in the contest. This issue requires serious, scientific user testing, not ad hoc tweaks.

Here are possible short-term mitigations:

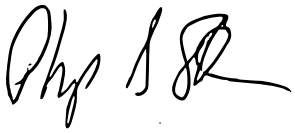
- Give every voter the option to hand-mark a paper ballot in person in every polling location. This can be accomplished by developing ballot-on-demand printers to accommodate the range of ballot styles and ballot languages Los Angeles elections require.
- Disable the BMD ballot box: use a traditional ballot box. This solves the autocast problem and the printhead problem. Provide ballot privacy sleeves for voters who need assistance carrying a ballot to a ballot box and casting it.

References:

- Appel, A., R. DeMillo, and P.B. Stark, 2019. Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3375755
- Bernhard, M., A. McDonald, H. Meng, J. Hwa, N. Bajaj, K. Chang, and J.A. Halderman, 2020. Can Voters Detect Malicious Manipulation of Ballot Marking Devices? *Proceedings of the 41st IEEE Symposium on Security and Privacy*. Preprint: https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf
- De Millo, R., R. Kadel, and M. Marks, 2018. What Voters are Asked to Verify Affects Ballot Verification: A Quantitative Analysis of Voters' Memories of Their Ballots. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3292208
- Stark, P.B., 2018. An Introduction to Risk-Limiting Audits and Evidence-Based Elections, Testimony to the California Little Hoover Commission, https://www.stat.berkeley.edu/~stark/Preprints/lhc18.pdf
- Stark, P.B., 2019. Ballot-marking devices (BMDs) are not secure election technology, letter to the Georgia House of Representatives Subcommittee on Voting Technology https://www.stat.berkeley.edu/~stark/Preprints/bmd19.pdf

- Stark, P.B., 2019. There is no Reliable Way to Detect Hacked Ballot-Marking Devices
  https://arxiv.org/abs/1908.08144
- https://vsap.lavote.net/wp-content/uploads/2019/09/VSAP_BMD-paper-path.pdf
- https://freedom-to-tinker.com/2018/09/14/serious-design-flaw-in-ess-expressvote-touchscreen-permission-to-cheat/
- https://freedom-to-tinker.com/2018/10/16/design-flaw-in-dominion-imagecast-evolution-voting-machine/
- https://freedom-to-tinker.com/2018/10/22/an-unverifiability-principle-for-voting-machines/
- https://securiosa.com/posts/how_the_expressvote_xl_could_alter_ballots.html

Sincerely,



Philip B. Stark