Addendum to Basic Security Requirements for Voting Systems

Wenke Lee, Ph.D.
Secure, Accessible & Fair Elections Commission

January 3, 2019

Background

Before the SAFE Commission meeting on December 12, 2018, I distributed a reference document to all Commissioners, which was: I.) a summary of basic security requirements for a secure voting system, II.) a comparison of the two main approaches under discussion (namely, hand-marked paper ballots versus a ballot-marking device with paper printouts), III.) a description of the current consensus among computer scientists that a voting system should be based on hand-marked paper ballots, and IV.) a proposal that the State of Georgia consider cost-effective measures, such as leasing – instead of purchasing – voting machinery.

Based on our discussions at the meeting and feedback from citizens, I would like to provide an addendum to that reference document, which includes: I.) a discussion of the requirements for a pre-certification audit following an election and the shortcomings of paper receipts from ballot-marking devices (BMDs), II.) a brief discussion that cybersecurity is always a central concern even with future technologies, III.) and clarification of a misunderstanding about election and voting system security.

I. Post-Election Audit: Avoid "Garbage-In, Garbage-Out"

At the SAFE Commission meeting in December, many Commissioners, as well as employees of the Secretary of State's Office, expressed support for the implementation of a formal election audit process. The purpose of a pre-certification election audit is to verify that the votes cast by voters are accurately captured and counted. The audit must verify the reported results, rather than merely test how the voting system performed. In the context of our current election system where votes are tallied by computers, an election audit can verify that automatically tallied results are correct prior to certification of the results – but only if a paper record exists.

A voting system must provide either a **human readable, post-vote paper receipt from a ballot-marking device** or an **actual paper ballot** as the durable, independent evidence that can be used as the authoritative source document in an audit or recount. Further, the paper record must have accurately captured the voters' intended votes, and the chain of custody of that paper must have remained secure after the ballots were cast by voters.

In order for paper receipts from a ballot marking device (BMD) to be useful in an audit, all of the following conditions must be met:

1) ALL voters must be WILLING to verify that each and every single vote that s/he cast with a BMD is clearly printed on the paper;
2) ALL voters must be ABLE to verify that each and every single vote that s/he cast with a BMD is clearly printed on the paper;
3) ANY voter who discovers a discrepancy is ENCOURAGED to speak up and BE ALLOWED TO VOTE AGAIN.

Unfortunately, to date, there is no systematic user study that has demonstrated that these conditions can be met. Quite to the contrary, studies and observations at polling stations have thus far suggested that a large percentage of voters do not carefully look at the printouts to verify that their votes have been printed on the paper correctly. Further, many voters cannot detect the discrepancies between votes they have cast with a BMD and errors on the printouts, especially for "down-ballot" races. And some voters do not feel comfortable to speak up if they discover a discrepancy, perhaps because they think such a discrepancy should not have happened so it must be their own fault. Some, wanting to maintain their right to a secret ballot, hesitate to disclose to poll workers who they intended to vote for and the specifics of the error.

These findings are not surprising at all because of human nature – not all of us are as diligent as we should be, many of us do not have the required memory capacity to remember all the votes we cast, and some of us would be embarrassed to inconvenience poll workers and fellow voters by asking to vote again.

In addition, it should be clear that it is not sufficient to have only some voters who are willing and able to verify their paper receipts. If receipts with erroneous votes are not identified (because some voters are not willing or unable), the post-election audit or recount will not produce an accurate result of votes cast by voters; and therefore, all voters are ultimately affected. For example, the audit may just confirm the tallied result from the voting system, which is incorrect because the BMDs had registered the votes incorrectly in the first place.

In summary, it is meaningless to perform a post-election audit on printouts that cannot be guaranteed to be valid in the first place; the audit would just be "garbage-in, garbage-out," and perhaps worse, give a false sense of accuracy or legitimacy of the election results.

Therefore, I believe it would be unwise, from a return-of-investment point of view, for the SAFE Commission to recommend that Georgia spend tens of millions of dollars to purchase a new voting system when, compared with the current system, the only major new feature would be paper receipts that cannot even be guaranteed to be valid and cannot be realistically audited.

Instead, once again, I recommend that we use the most accurate, safest, and most secure approach, which is to require a voter to hand mark his/her paper ballot, scan it, and drop it in a safe box. This is the most accurate method for voting because with hand-marked paper ballots, a voter both casts and verifies as they mark; it happens naturally and therefore human discipline and short-term memory play no role. This is the safest and most secure record for an audit because hand-marked paper ballots in a safe box have not been processed by any cyber

system and would not be vulnerable to any possible cyberattack. Although computerized scanners and tabulators are at risk of cyberattacks or errors, secure hand-marked paper ballots remain as the authoritative, auditable source documents for verifying computer-tabulated results. If errors are identified, paper ballots can be hand counted and the accuracy of the votes ultimately assured. That is not the case with BMDs: no authoritative hand count can be accomplished using BMD printouts that many voters are not able to verify.

Arguments for BMDs have been vocal and will likely continue. I recommend that we require vendors to provide evidence based upon rigorous, scientific studies that prove how BMD paper receipts would meet the requirements of a pre-certification election audit before they market their BMDs to Georgia. A rigorous study must involve a large number of representative, average voters using a mocked, complete ballot (i.e., including all, top to bottom, ballot races) similar to one from a recent major election, and must include printouts with erroneous votes (unknown to test subjects) to observe how willing and accurately voters will verify their votes. I also recommend that our decision-makers (e.g., legislators and state and county election officials) conduct similar rigorous studies using a proposed BMD system before they decide to purchase/deploy.

Further, even if BMDs are used, policy makers will need to plan for required feedback and mitigation procedures when voters identify BMD malfunction or errors. Is the equipment taken out of service? Are back-up units moved into place and planned for in the budget? Are paper ballots used from that point on?

All voters have the right to expect that their votes will be counted accurately. For a post-election audit or recount to be valid, all voters must have successfully verified that their votes have been accurately recorded on paper. If BMDs are used, the voters are in effect being required to use their memory skills to verify that BMDs did not make any errors. Why should voters be burdened to check the accuracy of voting systems? Isn't it the responsibility of the election officials and vendors to provide the appropriate systems and procedures to ensure that all votes will be counted accurately? More importantly, how do we guarantee the voting rights of all voters, regardless of their disabilities? In particular, if BMDs are used, how could we accommodate the large numbers of voters who do not have the memory skills to verify complex ballot content?

II. Future Technologies: Integrity/Security Is the Invariant

It always is dangerous to predict the future: who would have thought that we would be discussing a return to paper ballots in 2018? But we are here because of concerns about cybersecurity and its impacts on election integrity. Cybersecurity will be a constant concern, regardless of future technologies, and the likelihood of its manifestation will evolve with technology.

For example, it is tempting to think that in the near future we will adopt Internet-based (online) voting because young people simply will demand it. However, even if we can completely solve the user authentication problem to protect ballot secrecy, it is very challenging to guarantee

that a vote from a computer on the Internet is not the result of voter coercion/intimidation, vote buying, or malicious altercation.

On the other hand, we should have faith in our younger generations that -- despite their propensity for doing more and more activities online -- they will go to polling stations once they are educated about both a.) the importance of participating in our democracy and b.) the cybersecurity and vote integrity risks to online voting. Evidently, the very few countries that have experimented with allowing online voting have not seen an increase in voter participation (that is, there is no evidence that it enables more people to vote or satisfies a new voter preference). In fact, engaging with others at a physical polling place may actually promote a sense of pride and camaraderie among the public.

III. The System Is Not Connected to the Internet but It Can Still Be Hacked

It is easy to mistakenly believe that cybersecurity is all about Internet-facing security because after all, today most cyberattacks are coming from the Internet. However, as long as a computer accepts input data from another device (software or hardware) that is or has been part of an Internet-connected network, it can still be hacked via the Internet. For example, when an Internet-facing system is compromised, malware can embed itself in PDF, Word, and Excel files on the system, and these documents can eventually be loaded to a USB thumb drive. If this thumb drive then is used to share files among computers that are disconnected from the Internet, those computers can be infected by the same malware.

In fact, that is how advanced persistent threats (APTs) work: compromising an Internet-facing system, then leveraging data as it is transmitted to internal systems (e.g., via email or portable medium such as USB thumb drives) to infect greater parts of the system. A real-life example is the Stuxnet virus, which was able to infect controllers of Iran's nuclear machinery even though those controllers were not directly connected to the Internet or other networked computers.

In the context of election and voting systems, a ballot-marking device needs to be loaded with ballot data using a voting system memory card. The ballot data is formulated on another computer system, which is based on original data/documents, e.g., voter registration files and ballot programming files, that at some point came from an Internet-facing system. Therefore, even though a BMD or voting machine is not directly connected to the Internet, it still is under the threat of cyberattacks from the Internet or by individuals who have direct access to the computers.

Finally, we should not make the "failure to imagine" mistake again. We, as a nation, have failed to imagine how cyberattackers would manipulate our defense, healthcare, credit bureaus, and social media systems for malicious gain. Researchers already have demonstrated attack methods that can change votes recorded by a DRE or BMD. It requires no imagination to know that real attackers will try similar attacks on our election and voting systems. In the history of cybersecurity, researchers have tried to discover vulnerabilities, demonstrate new attacks, and urged vendors/industry to fix their vulnerable systems or practices. In the many cases where

responses by vendors/industry were not adequate, we ultimately have seen real attacks eventually surface and create havoc.

Summary

In order to ensure that an election and an audit is meaningful and accurate, we must have paper ballots that accurately capture the votes cast by voters. This in turn requires that, *if* BMDs are used, *all* voters are willing and able to verify a paper receipt (that is, a 100% voter compliance would be required). Studies thus far have shown that many voters are not willing or not able to do that, and it is unlikely that human nature can be changed. Therefore, printouts from BMDs cannot be used to guarantee a correct election or audit result. We should instead rely upon hand-marked paper ballots.

Cybersecurity will always be a central concern of voting systems. Never should convenience outweigh the need for better cybersecurity because without cybersecurity, there will be no election integrity.

We must secure all elements of the election and voting systems because even when a system is not directly connected to the Internet it can still be attacked by those who have direct access or via data that can be traced back to an Internet-facing system.