Lynn Garland   Bethesda, Maryland

I oppose the wireless networking of epollbooks on Election Day and therefore support this legislation.

As demonstrated in Iowa last week, election technology, even without hacking, can dramatically impair elections and reduce voter confidence in the outcome. Iowa was able to recover by counting the paper back up. But if Maryland's wireless network were hacked and the computer record of which voters had already voted were altered within the epollbooks, there would be no possibility of recovery. Iowa's system caused embarrassment but was resilient. Maryland's planned system is not resilient.

Implementing a wireless network for epollbooks may cause long lines, create unnecessary security risks, and is unnecessary. Computer scientists have argued again and again to keep election technology as simple and safe as possible and to avoid wireless connections where possible.

I am pleased that the SBE administration has decided to change its position and "not require" that any county use this election day wireless network of epoll books. But no county should use such a wireless network. Even one county's use of a wireless network can imperil the validity of election outcomes for all Marylanders and ruin voters' confidence.

The potential for the wireless network to cause long lines is not just hypothetical. During the relatively small-sized special election on Tuesday in District 7, the wireless networks caused the epoll books to slow down. Such a slow down would cause long lines in the upcoming 2020 elections, given the high participation expected.

Wireless systems are generally less secure than wired systems. Just last week, the National Institute for Standards and Technology, the entity that provides our federal government technical advice about voting systems, recommended banning wireless connections in future certified voting systems. Its rationale extends to epoll book systems. It said: Wireless connections can expand the attack surface of the voting system by opening it up to over-the-air attacks. Over-the-air access can allow for adversaries to attack remotely without physical access to the voting system. [i]

The security of any wireless system largely depends on the skill of those setting up and monitoring it. Hiring and training skilled technicians to correctly set up and support a wireless network at a handful of early voting sites is much more achievable

than hiring and training hundreds of skilled technicians for Election Day and expecting each of them to perform the tasks correctly.

This wireless network is unnecessary. The rationale for the system has changed over time. Initially, the SBE administration was planning a wireless network because the General Assembly was considering a same-day registration bill for Election Day that included address changes. As with early voting, if address changes were allowed, a wireless network would be needed to prevent voters from voting a regular ballot in multiple polling places. But then the General Assembly amended the bill to prohibit Election Day address changes, so there was no longer a danger that a voter could vote a regular ballot in multiple precincts. The law now specifies that on Election Day, citizens can only register in their own precincts based on where they reside. No wireless network is needed on Election Day to prevent voting in multiple polling places.

Nevertheless, the Board of Public Works was told that the wireless network was needed for same-day registration. And the members of the Board of Elections were told that the wireless network was needed to speed up the process for uploading the Election Day data from the epoll books to the registration system to prepare for the canvassing of the absentee ballots. The speeding up of the processing to have the information in time for the absentee canvass seems to be the current rationale for the wireless network.

On October 16th, 2019, I submitted a PIA request for documents related to the planning of the wireless network. The documents I received indicate that the need for the wireless network was not reevaluated after the bill was changed to eliminate same day address changes and that the original selection of the 6 largest counties was arbitrary. There is no indication that any analysis was done to support the contention that the 6 largest counties could not process the information in time for the absentee ballot canvass. Nor is there any indication that alternatives to a wireless network were considered.

HB 555 provides an alternative - - it offers counties the flexibility to slightly alter the start of the absentee ballot counting so that counties of any size will have ample time to process their data prior to the absentee ballot canvass and will not need a wireless network. This is the alternative - - safer and cheaper - - that I urge you to adopt.

---

[i] 14.2-D – <u>Wireless Communication Restrictions</u>
Voting systems must not be capable of establishing wireless connections
https://collaborate.nist.gov/voting/pub/Voting/VVSG20DraftRequirements/vvsg-2.0-2020-01-31-DRAFT-requirements.pdf