Senate Bill 831
Election Reform Act of 2021 INFORMATIONAL

Education, Health, and Environmental Affairs
March 3, 2021

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

I wish to comment on two parts of this Bill, one of which I strongly support and another that I do not support. I strongly support the use of internet ballot delivery by only those who need it (9.306, 1 and 2). I support allowing voters to choose whether they use ballot marking devices to vote, but I do not support *requiring* any voters to use ballot marking devices (3-303, A-2 and D-2).

Internet Ballot Delivery

Maryland's approach to internet ballot delivery is unintentionally, yet fundamentally, flawed and among the most insecure in the nation. The change implemented in SB831—restriction of the use of online ballot delivery—is urgently needed. In the absence of this restriction, Maryland opens itself to a variety of disruptions as the number of voters using online ballot delivery increases. Some of these disruptions could create far greater chaos than was witnessed last year in the Iowa caucuses[1].

There is no reason to believe that the vulnerabilities in the process have been exploited. But Maryland should make every effort to limit the use of online ballot delivery to those voters needing it. Maryland's legislators have had the benefit of advice from experts over the years; they now have the charge to secure Maryland's elections by passing this Bill.

Computer scientists have written to the Maryland State Board of Elections regarding internet ballot delivery since 2012; I have personally written and testified four times[2]. The SBE's overconfidence and disregard of our recommendations only increases its attractiveness as a

[1] Reid J. Epstein, Sydney Ember, Trip Gabriel and Mike Baker, "How the Iowa Caucuses Became an Epic Fiasco for Democrats", New York Times, Published Feb. 9, 2020. Updated Feb. 11, 2020. https://www.nytimes.com/2020/02/09/us/politics/iowa-democratic-caucuses.html as accessed on February 11, 2021.

[2] I wrote a letter, with others, to the SBE and several legislators on 15 January 2018 and another letter earlier to the SBE on 12 September 2016. I testified in person at the hearings for HB 0859, HB 706 and HB 1658 on 18 February 2020, 26 February 2019 and 27 February 2018 respectively, and earlier at a State Board meeting on 14 September 2016. Other computer scientists have sent letters earlier.

target. It is very easy for a bad actor to obtain thousands of voting credentials and request and complete thousands of online ballots from anywhere in the world. It is then trivial to have these ballots mailed in from within the US, and the State would not be able to distinguish fraudulent ballots from those completed by real absentee voters. If voters were to arrive to vote on Election Day and were told absentee ballots were requested on their behalf, there would be significant disruption.

Security technology alone cannot adequately address the possible acceptance of fraudulent votes made easy by the use of intermediating computers, weak authentication, stolen credentials, emailed ballot links and insecure computers used by voters. As more voters use the online ballot delivery system, the State becomes a more attractive target.

Further, in spite of a best practice requirement that signatures be used as the primary authentication mechanism for voted absentee ballots (see NIST IR 7711[3]), Maryland does not compare voter signatures for returned voted ballots. Note that absentee ballots delivered online—unlike ballots obtained at brick-and-mortar addresses or voted in person—may be obtained and cast in bulk by bad actors. The combination of online ballot delivery for all and the absence of a signature check makes it easier for a bad actor to illegitimately obtain and cast electronic ballots in bulk. The bad actor may be a nation state, or any domestic or international group or individual. Electronically-delivered ballots are delivered as internet links to email accounts; it is comparatively easy to set up fake email addresses in bulk.

A simple measure would greatly reduce Maryland’s vulnerability and SB 831 implements it by restricting the use of online ballot delivery. All other voters could still request their ballots using the online ballot request tool. Reducing the number of electronically-delivered ballots would reduce both the incentive for bad actors and the likelihood of significant chaos through fake absentee ballots.

The use of ballot-marking devices

Like all computational tools, ballot marking devices are vulnerable to both intentional alteration and error. While these errors can be detected if voters check the output of these devices, experiments have shown that voters do not check the output as carefully and as often as would be necessary. It is not thus reasonable to require voters to use ballot marking devices. It has been shown that voter education and a voting process that explicitly includes checking of the ballot helps increase voter detection of alteration of votes. I do not support

[3] "In most cases, any mechanism used to remotely authenticate voters will serve as a secondary method to authenticate returned ballots, with voter signatures generally providing the primary mechanism to authenticate returned ballots." NIST IR 7711, Sept 2011, "Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters".

requiring voters to use ballot marking devices, but if ballot marking devices are used by voters, they should be educated on errors and the process should include the explicit verification of the vote, including the provision of independent tools for those voters who cannot check ballots themselves.

Respectfully,

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

Note: affiliations are included for identification only

Poorvi L. Vora is Professor of Computer Science at The George Washington University. Her 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. She was a member of the team that deployed end-to-end-verifiable (E2E-V) voting system Scantegrity II in the Takoma Park elections of 2009 and 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. She obtained her Ph.D. from North Carolina State University. She has provided written and oral testimony to Committees of the Maryland Legislature on several Bills and have also provided oral and written testimony to the State Board of Elections.

APPENDIX: Interfering in an Election Using Online Ballot Delivery

A bad actor can easily obtain access to voter registration lists, voting records and the personal information required to register voters and/or request online absentee ballots. Thousands of online ballots can be obtained in one of many ways (some are listed below). The bad actor, using registered voters' credentials, downloads the online ballots, completes them through computerized ballot marking and prints them. All of this can be easily automated by software written for the purpose. The completed fake ballots would be mailed by humans. If, as a consequence, Maryland's counties received multiple ballots for many voters, they would have no way of distinguishing legitimate absentee ballots from fake ones, because *Maryland does not compare signatures for absentee ballots.*

Fraudulent Means of Access to Online Ballots

1. **Use credentials to impersonate <u>registered voters who vote regularly</u> and create chaos on Election Day**

Using the credentials for voters who vote regularly, the bad actor creates many thousands of fake email addresses, and then makes thousands of fake online absentee ballot requests to be sent to fake email addresses. All of this can be automated through software written for this purpose, and need not be done manually. Most of these voters will show up to vote on Election Day and will need to complete provisional ballots, which will create a great deal of chaos and distrust at the polls. By Maryland election law[4], if an absentee ballot has been received for this voter, both ballots will be rejected. If a voter does not show up to vote, neither they nor the State will know that a fraudulent vote was cast on their behalf.

2. **Use credentials to impersonate <u>registered voters</u> who vote infrequently and attempt to change the election outcome of a primary election**

Using the voter registration list and the credentials of voters who do not vote often in primaries, the bad actor would request internet delivered ballots by impersonating these voters and then complete and mail voted ballots. This could change the outcome of the primary. Some voters may show up to vote and would cast provisional ballots, but most will not and will not know a vote was cast on their behalf.

[4] COMAR: 33.11.05.04
.04 Ballot Rejection — Multiple Ballots from the Same Individual.
C. If an absentee ballot and provisional ballot are received from the same individual, the local board shall reject both ballots.

3. Send incorrect links to voters

Voters who have requested an internet delivered ballot in the past can be sent incorrect links by the bad actor, spoofing the local election board. Voters might follow instructions on what they believe to be a state website. They would then download their ballot from the fake website and mail it to the given address. Even if the given address were correct, their ballot would not be counted because they had never officially requested a ballot. Yet they would believe they had voted. There have been reports[5] that Russian actors explored the possibility of spoofing state election email accounts in 2016, though any such accounts were probably not used in 2016.

Impact on the voters who are impersonated by the software

a. Real voters showing up at the polls on Election Day will need to cast provisional ballots.
b. Voters who did not request absentee ballots and did not vote won't know that a vote was cast on their behalf.
c. Voters who did request and cast absentee ballots could have their vote replaced if the fake ballot is received after theirs. They too would not know their vote was replaced. If there were many instances of multiple ballots being received for a single voter, the state would investigate, however this would not be easy to resolve without contacting each voter and causing chaos and distrust.

The State cannot do much if fraud is suspected.

a. The State cannot distinguish between legitimate returned absentee ballots and fake ones.

b. The State cannot reassure real voters who voted with an absentee ballot obtained online that a fake ballot was not received after their legitimate ballot and counted instead. If two ballots were received, ostensibly from the same voter, the State may not be able to tell which one was genuine, especially without an intensive investigation.
c. The State will find it hard to reassure those voters who did not vote that a vote was not cast on their behalf. There will be considerable difficulty if a voter claims they did not cast a vote, but the State has a vote ostensibly completed by the voter, which is counted.

d. Moreover, a bad actor can create long lines and chaos at the polls merely by fraudulently requesting an online ballot, without having to vote and return those ballots. Because voters can mail absentee ballots up until midnight on Election Day. At the polls, the e-poll books will record that an absentee ballot has been requested and sent; and that annotation alone will require that the voter vote a provisional ballot.

[5] https://www.documentcloud.org/documents/3766950-NSA-Report-on-Russia-Spearphishing.html#document/p1 pg. 4

Voters can be targeted, based on the desired outcome.

a. If the bad actor wishes to **create chaos**, it would target those who vote often. In addition to being **terrible publicity** for the state, this would also **call into question a legitimate outcome**.

b. If the bad actor wishes to **change the election outcome without detection**, it would target unregistered voters and those who vote infrequently. Registering voters online is also easy, and the phony new registrations would be useful for subsequent election fraud.