1 April 2020

To

Governor Hogan, Maryland

Dear Governor Hogan,

I understand that the State Board of Elections has recommended that the upcoming special election and the postponed primary be vote-by-mail, and that you will be making a decision on the recommendation very soon.

As a scientist, I believe that it is critical for policy decisions to be informed by specialists. For this reason, I am pleased to see that the Board of Elections is taking seriously the input from state health officials and is recommending vote-by-mail as a means of protecting polling officials and voters from health hazards posed by COVID-19.

I have spent much of the last two decades studying voting system security. Hence, I feel compelled to point out two critical vulnerabilities in Maryland's approach to absentee voting and to suggest improvements.

- Unlike other states that vote by mail (Colorado, Washington, Oregon), and against best practice recommendations, Maryland does not compare voter signatures for returned voted ballots.
    - Because there is no way to authenticate a returned voted ballot, Maryland is not able to detect that a ballot was cast by someone other than the voter.
    - If both fraudulent and genuine votes are cast on behalf of a single voter, the State will not be able to tell which is which.
    - Large numbers of ballots could be fraudulently cast in the election, and the SBE would either not be able to tell that this kind of fraud had occurred, or end up creating chaos and generating distrust among voters by announcing that the fraud had been detected, but, when two ballots were received on behalf of a single voter, the State could not tell the two apart.
- Maryland allows all voters to receive ballots over the internet.
    - While these ballots need to be printed, completed and returned in person or by regular mail, internet delivery opens the election to a number of vulnerabilities. Voters can be sent incorrect links by software; they would

respond and incorrectly believe they had already voted. Another vote could be submitted on their behalf by the bad actor. There are other possibilities for disruption.

- The returned ballots are manually transcribed onto the requisite paper as the scanners do not take paper normally used by home printers or those in libraries and internet cafés. The transcription process is performed by paired volunteers and can hence result in election integrity and ballot secrecy violations. This year, it would also pose health challenges.

Maryland can take two simple steps to protect itself while it scales vote-by-mail to the entire state.

- Require the comparison of signatures with the existing signature on record and put into place procedures for informing voters of mismatches and allowing them to opportunities to correct it.
- Allow internet ballot delivery only for those voters who need it, such as voters with disabilities, UOCAVA voters and voters who are unable to receive ballots delivered by the postal system, or voters who did not receive them. Voters could self-certify that they need internet delivery on the form requesting an internet-delivered blank ballot.

Our intelligence agencies have warned us that US elections this year are very likely to be targeted by multiple possible bad actors. Additionally, Maryland is an attractive target because a bad actor can interfere in its elections without hacking into any part of its election technology. Computer scientists have written to the Maryland State Board of Elections regarding these problems since 2012; I have personally written and testified four times, including at least once to you. The SBE's overconfidence and disregard of our recommendations in the past only increases Maryland's attractiveness as a target. We had concerns when Maryland's absentee ballot rate was 5-6% of total ballots cast. In a vote-by-mail election, our concerns are heightened greatly.

I am very grateful for your leadership at this time of global crisis. I urge you to heed the call of those of us who have studied election security: please implement simple improvements to Maryland's absentee voting process to protect its elections. Please find attached more detail on the security vulnerabilities I summarized above; there is a website with details on our communication with the State as well[1]. I would be happy to

[1] https://www2.seas.gwu.edu/~poorvi/MarylandAudits/index.shtml#online-ballot-delivery

answer questions or meet virtually with any member of your team at any time to discuss this further or to provide any guidance within my expertise.

Respectfully,

Prof. Poorvi L. Vora

Professor, Department 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 focus has been on cryptographic end-to-end independently verifiable (E2E-V) voting systems and statistical election audits. She was a member of the team that deployed 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-V systems, and on information-theoretic models and measures of voting system security properties. She obtained her Ph.D. from North Carolina State University.

poorvi@gwu.edu

APPENDIX A: Problems With Online Ballot Delivery

Maryland's approach to internet ballot delivery is unintentionally, yet fundamentally, flawed. The flaws jeopardize both ballot secrecy and election integrity. Maryland opens itself to a variety of disruptions, not limited to undetected changes in election outcomes. Some of these disruptions could create far greater chaos than was witnessed recently in the Iowa caucuses[2]. Maryland's State Board of Elections (SBE), legislators and other elected officials have had the benefit of advice from experts over the years; the State now has the charge to avoid a major disruption of Maryland's vote-by-mail election.

Computer scientists have written to the SBE regarding internet ballot delivery since 2012; I have personally written and testified four times[3]. 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 because it does not compare signatures on received ballots! If multiple votes were received on behalf of a single voter, the later one is tallied by Maryland law, but that simply encourages a bad actor to vote late. In the event that an election outcome is very surprising, there would be significant disruption because the State could not be certain that the outcome was correct.

Suspected Russian interference in 2016 and the information released by Special Counsel Mueller in indictments[4], the report[5] and testimony[6] has added a great deal of urgency to

---

[2] 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 15, 2020.

[3] 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 which was copied to Governor Hogan. I testified in person at the hearings for HB 0859, HB 706 and HB 1658 on 20 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.

[4] U.S. v. Internet Research Agency, et al (1:18-cr-32, District of Columbia), 16 February, 2018. https://www.justice.gov/file/1035477/download as accessed on February 15, 2020.

[5] Special Counsel Robert S. Mueller III, "Report on the Investigation into Russian Interference in the 2016 Presidential Election", Volume I, parts II-C, III-A, III-B, III-C, March 2019. http://www.justice.gov/storage/report.pdf As accessed on February 15, 2020.

our concerns. Maryland is an attractive target because Maryland has a statewide voting system; and a bad actor can target its elections without hacking into any part of its election technology. Our intelligence agencies advise that Russian efforts to interfere in our elections are increasing in intensity over time, and the interest in Maryland's servers and in ByteGrid appear very much like tests to assess the State Board of Elections' readiness to protect its elections. The SBE's overconfidence and disregard of our recommendations in the past only increases Maryland's attractiveness as a target.

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.

Maryland is among only three states that have allowed all voters to receive blank ballots online. However, in spite of a best practice requirement that signatures be used as the primary authentication mechanism for voted absentee ballots (see NIST IR 7711[7]), Maryland does not compare voter signatures for returned voted ballots. This 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.

Two simple measures would greatly reduce Maryland's vulnerability: restricting the use of online ballot delivery to those who need them and comparing signatures on all received voted ballots. These measures would reduce both the incentive for bad actors and the probability of significant election fraud through fake absentee ballots.

---

[6] Washington Post Staff, "Transcript of Robert S. Mueller III's testimony before the House Judiciary Committee", July 24, 2019. https://www.washingtonpost.com/politics/transcript-of-robert-s-mueller-iiis-testimony-before-the-house-judiciary-committee/2019/07/24/7164abfe-ad96-11e9-a0c9-6d2d7818f3da_story.html As accessed on February 15, 2020.

[7] "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".

APPENDIX B: Attacks Enabled by 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 no other ballot is received, these ballots would be accepted and counted as legitimate because Maryland's counties have no way of distinguishing legitimate absentee ballots from fake ones, because astonishingly, *Maryland does not compare signatures for absentee ballots!*

Fraudulent Means of Access to Online Ballots

1. **Use credentials to impersonate registered voters**

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. By Maryland election law[8], if more than one absentee ballot has been received for this voter, the later one will be accepted. If a bad actor casts a late internet-delivered ballot, neither the voter nor the State will know that a fraudulent vote was cast on the voter's behalf.

2. **Use credentials to impersonate unregistered voters, register them, request and vote online ballots**

Once the voter registration is completed, a postcard may be sent to the original address, and a voter may notice it, but not many are likely to draw the State Board's attention to this. Most will not know a ballot was cast on their behalf. A copy of the voter's driver's license or ID is required, but such information is easy for the bad actor to obtain online,

[8] COMAR: 33.11.05.04
.04 Ballot Rejection — Multiple Ballots from the Same Individual.
B. If more than one ballot is received from the same individual in different envelopes:
(1) If the signed oaths have different dates, only the ballot with the later date shall be counted;

considering the fact that doctors, dentists, lawyers and gyms often store copies of driver's licenses of their patients/clients/customers.

3. Send incorrect links to voters

Voters, whether they requested an internet-delivered ballot or not, could 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. The given address could be incorrect or the ballot itself could be incorrect. Yet they would believe they had voted. There have been reports[9] that Russian actors explored the possibility of spoofing state election email accounts in 2016, though any such accounts were probably not used in 2016. Even if the SBE detected such efforts because they received too many incorrect ballots, or too many ballots from voters who did not request internet delivery, and made voters aware of such attacks, it would have a large impact on voter confidence.

Impact on the voters who are impersonated by the software

a. Voters who did not request absentee ballots and did not vote won't know that a vote was cast on their behalf.

b. 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

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

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.

Voters can be targeted, based on the desired outcome.

a. If the bad actor wishes to **create chaos**, it would send fake ballots to voters who would vote them and the SBE would obtain ballots that were clearly fake and would have to be rejected, and the public informed.

b. If the bad actor wished to **change the election outcome without detection**, it would target voters supporting a particular candidate and change their vote, submitting the voted ballot as close as possible to the deadline and replacing the voter's legitimate vote. Registering voters online is also easy, and the phony new registrations would be useful for subsequent election fraud.

APPENDIX C: The Context

As mentioned in the main body of this statement, computer scientists have been writing to the State Board of Elections regarding this issue since 2012. Most recently, in 2016, one of us also presented these concerns in person at an SBE meeting. Since then, it has been reported that US intelligence agencies believe Russia attempted to interfere in the 2016 elections, and its efforts are expected to increase in intensity and capability in future elections. I have also testified in person to the House Ways and Means Committee at the hearings for HB 0859, HB 706 and HB 1658 on 20 February 2020, 26 February 2019 and 27 February 2018 respectively.

Foreign actors, thought to be Russians, attempted to breach online voter registration databases throughout the US in 2016, and the FBI found that they were successful in doing so in at least one state. Additionally, thousands of fake social media accounts were created and successfully created and operated. While the state of Maryland detected attempts to breach its online voter registration database, officials have testified that they believe the attempts were not successful. But it is not possible to categorically state that a security breach did not occur, because it is relatively easy for competent attackers to hide their trail. Large organizations with considerable resources have been subject to data breaches. (Examples include Equifax, the US Government's Office of Personnel Management, Adobe, Sony, Capital One, Yahoo, Target, Marriott, the University of Maryland, Anthem Health Insurance). It typically takes many months for an organization that does not immediately detect a breach to become aware of it. There are likely many organizations that are successfully breached but never detect the breach.

Any online voter registration database, including Maryland's, can be breached, and it is likely to be a while before the breach is discovered, if ever. Additionally, some attacks do not require the hacking of Maryland's election technology. For example, as with social media accounts, the creation of fake email accounts in bulk is very easy.

The Ease of Obtaining Credentials

The personal information required to request and download an absentee ballot in Maryland (such as driver's license number or birth date) is no longer sufficiently confidential for voter authentication.

- All the information is easily available on the "dark" market—consider the description, in the Mueller indictment of 16 February, of Russians using the social security numbers of real US citizens in order to open bank accounts[10].

- It is also shared legitimately and widely among law enforcement agencies, universities, doctors' offices and hospitals, and hence could be leaked (or may already have been) through data breaches of these entities.

- Additionally, the recent hacks of credit agency Equifax and the federal Office of Personnel Management (OPM) revealed considerably more "secure" information on a huge number of US voters and are believed to have been carried out by a state actor. Because this information is not yet on the "dark" market for personal gain, it is suspected to have been obtained for some other purpose appropriate for a state actor.

- Finally, ByteGrid servers stored the credentials of all Maryland voters, and an interested ByteGrid insider could have obtained access to all the credentials without leaving a trail.

In fact, reliance on personal data alone to authenticate a voter is never sufficient for any high security activity like voting, and changing the type of data required will not solve this problem.

The Ease of Obtaining and Completing Ballots in Bulk

It is not hard to automate access, download and completion of online ballots. The Mueller indictments describe how Russian trolls from a single company opened and ran

[10]"In or around 2016, Defendants and their co-conspirators also used, possessed, and transferred, without lawful authority, the social security numbers and dates of birth of real U.S. persons without those persons' knowledge or consent. Using these means of identification, Defendants and their co-conspirators opened accounts at PayPal, a digital payment service provider; created false means of identification, including fake driver's licenses; and posted on ORGANIZATION-controlled social media accounts using the identities of these U.S. victims. Defendants and their co-conspirators also obtained, and attempted to obtain, false identification documents to use as proof of identity in connection with maintaining accounts and purchasing advertisements on social media sites", page 16, para 41, *ibid*.

hundreds of email and social media accounts[11], pretending to be US citizens. The company's annual expenditure was in the millions of dollars[12].

- "Tests" to differentiate humans from software are not very effective—consider that the Russians are believed to have created many thousands of fake social media accounts that are operated by software, behave like human participants, and exist solely for the purpose of interfering in the US election.
- It is also easy to make fake ballot requests appear to come from different IP addresses, spaced out over time, with an extremely large number being made close to deadlines, making it harder to detect them or respond effectively.
- The Mueller indictment describes how Virtual Private Networks (VPNs) and computer infrastructure in the US[13] were used to disguise the computers and the location of those opening and using the accounts.

The Ease of Casting Illegitimate Ballots in Bulk with Online Ballot Delivery

The fact that bulk impersonation attacks have not been detected in Maryland in the past does not mean they did not happen or that they will not happen in the future. A determined actor could easily obtain bulk access to virtual ballots delivered online. Information on who votes regularly and who does not is also easily available and can be used to focus attention on those who do not vote often and hence would not know an online ballot was obtained on their behalf. To prevent fraudulently-obtained ballots from being cast, and in order to ensure that a voted ballot received by the election authority was indeed sent by the voter, the State should check signatures, which it does not. So there is no way of determining whether a received, voted absentee ballot was indeed cast by the voter.

---

[11] "Defendants and their co-conspirators also registered and controlled hundreds of web-based email accounts hosted by U.S. email providers under false names so as to appear to be U.S. persons and groups", pg. 16, para 40, *ibid*.

[12] "The ORGANIZATION [Internet Research Agency] employed hundreds of individuals for its online operations, ranging from creators of fictitious personas to technical and administrative support. The ORGANIZATION's annual budget totaled the equivalent of millions of U.S. dollars", page 5, para 10(a), *ibid*.

[13] "Defendants also procured and used computer infrastructure, based partly in the United States, to hide the Russian origin of their activities and to avoid detection by U.S. regulators and law enforcement", page 3, para 5, *ibid*.

Potential Impact

In the worst case, such fraud would change the outcome of the election but would not be detected. On the other hand, if fraud is suspected, because some contest outcomes are very different from those expected, it will take a while to determine that fraud did occur, and to determine what the correct election outcome is. Voters not paying much attention to their mail might find out on Election Day that the State received a change of address on their behalf and believes they live elsewhere; hence they are not eligible to vote in the jurisdiction they live in. Election officials will be hard pressed to explain why they ignored several letters from computer scientists urging them to address the core problem. This will easily surpass the problem faced by the Democratic Party in Iowa.

The use of online ballots poses many other problems as well: online ballot marking reveals the vote to any malware on the voter's computer; mailed ballots have to be reproduced by hand on ballot stock requiring a large number of expended person hours and uncertainty regarding whether the vote was reproduced correctly; the return rate of ballots delivered online is smaller than that for ballots delivered by the postal system.