House Bill 1658
Election Law – Absentee Ballot Requests, Delivery, and Marking
SUPPORT

Ways and Means
February 27, 2018

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

Micah Sherr
Provost's Distinguished Associate Professor
Department of Computer Science
Director
Georgetown Institute for Information Assurance
Georgetown University

The security weaknesses of Maryland's approach to absentee ballots and ballot marking greatly impact Maryland voters. Because this approach is used in federal elections, its weaknesses also pose national security concerns and impact other US citizens. Unintentional, fundamental conceptual flaws in the approach jeopardize both ballot secrecy and election integrity. These flaws cannot be addressed by securing the SBE server and tool software, and need the change implemented in HB 1658: **restriction of the use of online ballot delivery and ballot marking to voters with disabilities and military and overseas voters**.

Computer scientists have written several times on this issue to the State Board of Elections[1]. The two of us were among computer scientists who wrote to the Board and several state legislators earlier this year. Much of what we wrote in the letter this year is included in this written testimony.

Problems with the current approach to online ballot delivery: Maryland is among only three states that allow 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[2]), the State does not check voter signatures on returned voted ballots. This makes it easy 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

---

[1]Most recently, on or about 15 January, 2018 Profs. Vora and Sherr wrote a letter, with others, to the SBE and several legislators; Prof. Vora wrote a letter to the SBE with others on 12 September 2016; Prof. Vora testified in person at a State Board meeting on 14 September 2016; other computer scientists have sent letters earlier.

[2]"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".

individual. **The state of Maryland is hence among the most vulnerable in the US to major election tampering. Because the bad actor need not hack into any part of the State's technology to carry out election fraud (we describe some fraud scenarios below), Maryland's vulnerability cannot be addressed by focusing only on securing its technology.**

Problems with the current approach to online ballot marking: ***ballot secrecy cannot be protected when votes are entered into personal computers on the internet***. Personal computers are known to be particularly vulnerable to malicious software. Votes may be exposed to employee surveillance software, spyware or viruses unintentionally installed by voters or other users of the computer. Through these, entities that would never have had the opportunity to determine individual votes, because of lack of physical access, could now have virtual access at a large scale from anywhere in the world. Well-intentioned efforts by Maryland to secure its software and server cannot secure the voter's computer, where the vote is first entered.

A simple measure would greatly reduce Maryland's vulnerability and HB 1658 implements it. It restricts the use of online ballot delivery and ballot marking to voters with disabilities and military and overseas voters. All other voters could still request their ballots using the online ballot request tool. The ballots would be delivered as paper ballots to their physical addresses, and not as internet links sent to their email accounts. The comparative difficulty of using fake physical addresses in bulk over using fake email addresses will substantially reduce both the incentive for bad actors and the probability of significant election fraud through fake absentee ballots.

Computer scientists have been writing to the Maryland State Board of Elections regarding this and related issues since 2012. Both of us were among those who wrote to the SBE and state legislators earlier this year. Suspected Russian interference in 2016, and the information in the material released by Special Counsel Mueller in the indictment[3] of Internet Research Agency and others has added a great deal of urgency to our concerns. The possibility of online ballot delivery being exploited to cast fraudulent votes can no longer be dismissed as abstract or theoretical.

Consider the following scenario. For more detail, please see the Appendix.

1. A bad actor obtains access to voter registration lists, voting records and the personal information required to register voters and request online absentee ballots. 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

[3]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

US citizens in order to open bank accounts[4]. 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.

2. The bad actor then creates many thousands of fake email addresses, makes thousands of fake online absentee ballot requests to be sent to fake email addresses, 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 Mueller indictments describe how Russian trolls from a single company opened and ran hundreds of email and social media accounts[5], pretending to be US citizens. The company's annual expenditure was in the millions of dollars[6].
    a. "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.
    b. 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.
    c. The Mueller indictment describes how Virtual Private Networks (VPNs) and computer infrastructure in the US[7] were used to disguise the computers and the location of those opening and using the accounts.
3. Alternately, the bad actor can write malware for voters' computers that would access the ballot when the voter downloads it, complete the ballot, and secretly transmit the

[4] "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*.

[5] "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*.

[6] "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*.

[7] "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*.

now voted ballot over the internet to the bad actor's server. The voter, who is unaware of the attack, might also complete and mail the ballot.

4. The completed fake ballots are finally mailed by humans. 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 *Maryland does not check signatures on absentee ballots!***
5. Impact on the voters who are impersonated by the software:
    a. Real voters showing up at the polls on Election Day will be furious that their ballots must be provisional.
    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.
6. If fraud is suspected because of the chaos on election day:
    a. How will the state distinguish between legitimate returned absentee ballots and fake ones?
    b. How will the state 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, how would anyone tell which one was genuine?
    c. How will the state reassure those voters who did not vote that a vote was not cast on their behalf? What happens if it was?
7. The bad actor can choose which voters to target, 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.
8. Other mischief is possible: voter addresses can be changed online, and voters – who may not pay sufficient attention to postcards informing them of the change – would arrive at the "wrong" location on Election Day. Voters can be sent incorrect links by the bad actor, spoofing the local election board, and might follow instructions on what they believe to be a state website, giving up valuable information in the process. They would believe they mailed in a ballot to the state when they did not. There have been reports that Russian actors explored such a possibility in 2016, by setting up fake email accounts

intended to spoof state election email accounts, though any such accounts were probably not used in 2016.

In the event that the Bill does not pass, and any of the above takes place, how will the Legislature and the SBE explain why they ignored repeated warnings from computer scientists?

We understand and applaud the desire to improve voter services, but all voters suffer when elections are interfered with. **We urge you to pass this Bill.**

Respectfully,

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

Prof. Micah Sherr
Provost's Distinguished Associate Professor, Department of Computer Science,
Director, Georgetown Institute for Information Assurance
Georgetown 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 end-to-end independently verifiable (E2E) voting systems which enable voters and observers to audit election outcomes without requiring them to rely on the trustworthiness of election technology or unobserved election processes. Prof. Vora was a member of the team that deployed polling-place, paper-ballot-based, E2E voting system Scantegrity II in the Takoma Park elections of 2009 and 2011, and of the team that developed remote voting E2E system Remotegrity and accessible voting variant Audiotegrity, used in 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.
poorvi@gwu.edu

Micah Sherr is Provost's Distinguished Associate Professor in the Computer Science Department at Georgetown University and director of the Georgetown Institute for Information Assurance. His academic interests include privacy-preserving technologies, electronic voting, wiretap systems, and network security. He participated in two large-scale studies of electronic voting machine systems, and helped to disclose numerous architectural vulnerabilities in U.S. election systems. His current research examines the security properties of legally authorized wiretap (interception) systems and investigates methods for achieving scalable, high-performance anonymous routing. Micah received his B.S.E., M.S.E., and Ph.D. degrees from the University of Pennsylvania. He is a recipient of the NSF CAREER award.
msherr@cs.georgetown.edu

APPENDIX

The Context

As mentioned in the main body of this letter, 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.

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, Yahoo, 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 Casting Illegitimate Ballots in Bulk with Online Ballot Delivery

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. The information is widely and cheaply available on the black market and through "dark" Internet sites. 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. Fraudulent requests for absentee ballots can be made in bulk by using this information. Following the recent data breach at credit reporting agency Equifax, no personal data can be assumed to function as a secure credential. 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 fact that bulk impersonation attacks have not been <u>detected</u> in Maryland in the past does not mean they did not happen or that they will not happen in the future. As described in the

main body of the letter, 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.

Maryland's well-intentioned efforts to secure its software and server can, at best, protect the information and votes it holds. The state cannot address the entry of fraudulent votes made easy by the use of intermediating computers, weak authentication, 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.

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 on Election Day, because many voters show up to vote but have absentee ballots cast in their names, 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. If provisional ballots are cast, these will not be tallied toward the outcome announced on the evening of Election Day. Additionally, election officials will be hard pressed to explain why they ignored several letters from computer scientists urging them to address the core problem.

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.