14 September 2016

Chairman McManus, Vice-Chair Hogan, State Board of Elections Members, Members of the Public,

Thank you for the opportunity to address you today.

I am Poorvi L. Vora, a tenured Professor of Computer Science at The George Washington University. I have published extensively on the subject of voting system security, have a doctorate in electrical engineering from North Carolina State University, and a master's in mathematics from Cornell.

What I will say today is informed by my research and does not necessarily reflect the views of my employer, collaborators or sponsorship agencies, the National Science Foundation and the Maryland Procurement Office.

The security weaknesses of the online ballot marking tool, and its proposed expanded use, greatly impact Maryland voters. Because the tool will be used in federal elections, its weaknesses also pose national security concerns and impact other US citizens like me. 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.

First, 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.

Second, weak credentialing jeopardizes the integrity of the election outcome. The information required to make an absentee ballot request is available in bulk on the black market, or spread widely among law enforcement agencies, doctors' offices and hospitals. Perpetrators of bulk fraudulent requests using the information can evade detection because it is trivial to establish multiple email addresses, and IP addresses can be changed easily. Even without the information, emailed passwords can be accessed by third parties and used to cast votes in bulk. Maryland's well-intentioned efforts to secure its software and server can, at best, protect the votes it holds. They cannot address the entry of fraudulent votes unintentionally made easy by the use of intermediating computers, weak authentication and emailed passwords. As more voters use the system, it becomes a more attractive target. The fact that attacks have not been detected in the past does not mean they will not happen in the future.

At best, securing the server and the software is like locking the ballot box, while malicious actors may stuff it, undetected, and voters may be spied upon, without their knowledge, as they fill their ballots.

While I applaud your efforts to improve voter services, I urge you to restrict the use of ballot marking software to voters disadvantaged without it, and to restrict the delivery of online ballots to those for whom such delivery is required by federal law.