I am Poorvi L. Vora, a tenured Professor of Computer Science at The George Washington University, and have published extensively on the subject of voting system security. I support this Bill.

It is grossly negligent for the State of Maryland to continue its current approach after the Mueller indictments, which describe a Russian company carrying out all the activities necessary to perpetrate online absentee ballot fraud at significant scale in Maryland. With its current absentee voting process—which includes electronic delivery of absentee ballots to all who request them—the State is among the bottom three states in the US on the issue of absentee ballot security, and hence a very vulnerable target.

Accurate personal information is easily found in the dark market. We do not know if the foreign entities with ownership in ByteGrid made copies of the voter information on their servers while they were providing election services to Maryland. Using personal information on voters, it is easy to impersonate them and request online ballot delivery to fraudulent email accounts. The ballots can then be printed, completed and mailed. These requests and completed ballots would appear legitimate to the State because they would use authentic credentials. It is trivial to hide IP addresses, preventing the identification and tracking of requesting computers and their locations. Those who say they will detect such requests, but need to keep their detection techniques secret, are voicing a misplaced overconfidence.

Bad actors could target regular voters, in which case many voters would show up on Election Day to find a vote had been cast on their behalf and they would have to vote provisionally, creating a lot of confusion and distrust. Or they could target voters who do not vote often, and attempt to change election outcomes, especially for primary elections. Or they could target unregistered voters, register them and then vote for them. Or they could provide false links to voters and lead them to believe they had voted, while they had merely given up their credentials to the bad actor. The list goes on.

There is no technical means available to prevent such attacks. This Bill makes an important change that reduces the attack surface, thus limiting the amount of possible damage, and, with that, the incentive to bad actors to go through the effort of carrying it out. It allows for exceptions in unusual circumstances. This change disenfranchises no voters. It benefits all, because all would suffer were such an attack to occur.

47 other states in the US already have similar, or stronger, restrictions. Students who have taken an introductory undergraduate level computer security class have the expertise necessary to carry out the attacks. It would be crazy for Maryland to not pass this Bill. Much of what we have been warning the State about over the years has happened in the last two years. If this Bill does not pass, and any of the above scenarios comes to be, how will the Assembly justify ignoring repeated warnings from computer scientists?