September 12, 2016

David J. McManus, Chairman
Patrick J. Hogan, Vice Chairman
Bobbie S. Mack
Michael R. Cogan
Kelley A. Howells

Dear Chairman McManus, Vice-Chair Hogan, and State Board of Elections Members:

Recent revelations, such as the hacking of the DNC and the voter registration databases of Arizona and Illinois, have increased concerns about cyber threats to our elections. In addition, credentials of many Maryland citizens may have been compromised by a number of high profile hacks, including the Office of Personnel Management (OPM), the University of Maryland, and Anthem Health Insurance, to name just a few.

Consequently, we are writing once again to share with you our concerns about Maryland's proposed expansion of Internet-based voting-related services. We applaud the state's continuing efforts to make voting more accessible. However, the specific combination of online services you plan to offer any absentee voter combined with the extremely weak log-in (authentication) information required to access those services will make Maryland one of the most vulnerable states in the U.S. for major election tampering. All systems connected to the Internet are under constant bombardment from a diverse and growing range of attacks that even hardened government, military, industrial, and financial institutions are finding increasingly difficult to ward off. Because you administer federal elections, this is an issue that affects our national security.

Maryland still has not solved the critical problem about which we initially contacted you in September, 2012: There must be a secure method for authenticating voter transactions that guarantees that the reliably identified voter, as opposed to a bad actor or piece of malicious software, is at the other end of the transaction. Maryland's authentication method remains extremely weak by any commonly accepted standard of cyber security. Until a much more robust authentication process is in place, it is unwise to expand the services offered.

Strong authentication must rely on information that is *secret*. But the log-in information Maryland requires is simply not secret. Social Security numbers are widely available in bulk on the black market; we have heard quoted prices such as 9 to 10 cents per ID package (name, address, birth date, SSN, driver's license number, and other identifying data), sorted by zip code. The breach of the University of Maryland's computer system may have added another 300,000 potential victims to that pool. The remaining identifier chosen by the State Board of Elections is the issue date of the driver's license/MVA ID. This information is not closely held, since tens of thousands of employees of state and local law enforcement agencies as well as MVA staff, doctors' offices, and hospitals have ready access to it.

Email is not a secure medium. The sender of an email is easily forged, and there is no good way to provide end-to-end encryption for email between voters and election officials. Consequently, sending sensitive information such as passwords via email has been likened to taping a $20 bill to a postcard and expecting it to arrive at its destination intact. But unlike a lost greenback, it will not be possible to detect that information in the email had been copied or tampered with *en route*.

Once a voter's identifying information is acquired, an attacker could request an absentee ballot, have it delivered to an email address provided by the attacker, and either download it or mark it online. All of these steps could be accomplished using automated scripts that would allow a bad actor to launch attacks on a scale that would not be feasible with traditional paper absentee ballots. Even the safeguard of requiring the downloaded, printed ballot to be mailed with a signed oath would offer no protection, since voter signatures are not checked in Maryland and for some categories of voters may not even be on file.

The risk of fraudulent ballot requests is not theoretical. In 2013 Jeffrey Garcia was sentenced jail in Florida for making over 2500 fraudulent online ballot requests. Furthermore, just because a hack hasn't been detected doesn't mean it hasn't occurred. Scanning the State Board of Election's computer systems for intrusions is not sufficient. We know that successful attacks typically are not uncovered until months after the initial break-in, as we've seen with the DNC hack. As more voters use the online system, opportunities for hackers increase in size and relevance.

The Presidential Commission on Election Administration noted that election fraud is most commonly attempted and accomplished using absentee, rather than in-person, voting. The proposed system, combined with the weakness of the safeguards currently in place, would make Maryland an extremely attractive target. Large scale fraud would be harder to detect, prevent, or prosecute than traditional absentee ballot schemes.

The insecurity of the Internet also raises issues about ballot secrecy. Under the current system voted ballots are sent back to the State Board of Elections server, thereby threatening the secrecy of the ballot. Even if the online ballot marking system itself does not record or store any information that might associate a specific voter with his or her ballot selections, it is still possible for this information to be collected and stored by third parties without the voter's knowledge. Voters marking their ballots on machines or networks that are not their own, such as computers in the workplace or in libraries, are vulnerable to malware that may silently transmit copies of their marked ballots to a third party. Similar malware could infect voters' personal computers or mobile devices. No activity that takes place on an Internet-connected device, especially an unsecured one such as a voter's private computer, can be guaranteed to be secret.

Because of the scale of attacks that would be possible if Maryland allows *all* voters to request, receive via email, and/or mark absentee ballots online, we strongly urge you to reconsider this approach. Most Maryland voters have no need to receive ballots online; traditional paper

ballots mailed to voters provide most of the same convenience as online delivery and have the advantage of providing voters with an envelope for returning the ballots. Likewise, marking ballots on an Internet-connected device, which provides no value to most voters – including military voters – over hand marking, invites malicious transmission of a copy of the voted ballot to a third party. Since the size of a potential target is a huge factor in its vulnerability to fraud, we recommend that you restrict online ballot delivery to as small a population as possible, specifically those for whom such delivery is legally mandated, namely military and overseas voters and voters with disabilities.

Though we very much support your goal of finding new, innovative ways to engage more voters in the election process, we are sadly all too familiar with the dangerous environment into which you are introducing these new services. We urge you to proceed with extreme caution lest you inadvertently put the integrity of Maryland's elections at grave risk.

Please let us know if there is any way we may be of help.

Respectfully,

Prof. J. Alex Halderman
Professor, Department of Computer Science and Engineering, the University of Michigan
jhalderm@eecs.umich.edu

Dr. David R. Jefferson
Visiting Scientist, Lawrence Livermore National Laboratory
D_jefferson@yahoo.com

Dr. Barbara Simons
IBM Research (retired); Former President, ACM (Association for Computing Machinery)
simons@acm.org

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

Note: affiliations are included for identification only.

J. Alex Halderman is Professor of Computer Science and Engineering at the University of Michigan and Director of Michigan's Center for Computer Security and Society. His interests include computer and network security, Internet security measurement, censorship resistance, and electronic voting, as well as the interaction of technology with law and international affairs. Named one of Popular Science's "Brilliant 10" for 2015, his recent projects include ZMap, Let's Encrypt, and the TLS Logjam and DROWN vulnerabilities. A noted expert on electronic voting security, Prof. Halderman helped demonstrate the first voting machine virus, participated in California's "top-to-bottom" electronic voting review, and exposed election security flaws in

India, the world's largest democracy. When Washington DC invited the public to test its pilot Internet voting system, Halderman demonstrated security vulnerabilities that would allow malicious entities to add and replace votes. His analysis received national attention and resulted in DC's decision not to use the system. In 2015, he received the Alfred P. Sloan Fellowship, which is awarded to "early career scientists and scholars of outstanding promise" "in recognition of distinguished performance and a unique potential to make substantial contributions to their field". He holds a Ph.D. from Princeton University.

David Jefferson is an internationally recognized expert on voting systems and election technology, and an advisor to five successive California Secretaries of State. In 2004 he was coauthor of the SERVE Security Report detailing the security vulnerabilities in the Defense Department's proposed Internet voting system, leading to the cancellation of the program. In 2003 he was a member of the California Task Force on Touchscreen Voting, whose recommendations led to voter-verified paper audit trails for electronic voting machines. He has led half a dozen technical studies on reliability and security of voting systems, including the California Post-Election Audit Standards Working Group that produced the first government study of post-election auditing. He serves on the boards of directors of both the California Voter Foundation and Verified Voting. Jefferson received a Ph.D. in computer science from Carnegie-Mellon University. From 1980 to 1994 he was a computer science professor at USC and then at UCLA, and now works at Lawrence Livermore National Laboratory where he is involved with research in supercomputing and cyber security.

Barbara Simons published *Broken Ballots: Will Your Vote Count?,* a book on voting machines co-authored with Douglas Jones. She has served on the Board of Advisors of the U.S. Election Assistance Commission since her appointment in 2008, and she co-authored the report that led to the cancellation of Department of Defense's Internet voting project (SERVE) in 2004 because of security concerns. She was a member of the National Workshop on Internet Voting that conducted one of the first studies of Internet Voting and produced a report in 2001. She co-authored the July 2015 report of the U.S. Vote Foundation entitled *The Future of Voting: End-to-End Verifiable Internet Voting.* Simons co-chaired the ACM (Association for Computing Machinery) study of statewide databases of registered voters, and co-authored the League of Women Voters report on election auditing. Simons is a Fellow of ACM and of the American Association for the Advancement of Science. She has received several awards, including the Distinguished Engineering Alumni Award from the College of Engineering of U.C. Berkeley, where she obtained her Ph.D. in computer science. She chairs the Board of Directors of Verified Voting and is retired from IBM Research.

Poorvi L. Vora is Professor of Computer Science at The George Washington University (GW). Her research focus is in the area of the design of secure voting systems; a large part of her research has been sponsored by the National Science Foundation. She has worked with the National Institute of Standards and Technology on definitions of desired properties of end-to-end-verifiable voting systems, and on information-theoretic models and measures of voting system security properties. Her research papers have been presented and published at the best venues for voting system security research, and she has given several invited academic

presentations on voting system security. Before GW she worked for eight years at Hewlett-Packard in many capacities in HP Laboratories and the product divisions, including as Security Architect in the Office of the CTO of Imaging and Printing. She has a Ph.D. from North Carolina State University, and serves on the Board of Advisers of Verified Voting.

Cc: Governor Larry Hogan
Attorney General Brian Frosh
Sen. Joan Carter-Conway, Chair, Education, Health & Environmental Affairs Committee
Del. Sheila E. Hixson, Chair, Ways and Means Committee
State Administrator of Elections Linda H. Lamone
Deputy State Elections Administrator Nikki Charlson
Assistant Attorney General Jefferey L. Darsie