September 25, 2012

Robert L. Walker, Chairman
Bobbie S. Mack, Vice Chairman
Rachel T. McGuckian
David J. McManus, Jr.
Charles E. Thomann

Maryland State Board of Elections
151 West Street, Suite 200
Annapolis, MD 21401

Honorable Chairman Walker and Esteemed Board Members:

We are computer science researchers with election technology expertise. We strongly support your goal of using the Internet to increase the convenience of voter registration and registration changes for both voters and election officials. As with all technological innovations, implementation details can determine the integrity of the online registration process.

Regrettably, we have identified severe security vulnerabilities in Maryland's online voter registration system. These problems leave the system open to large-scale, automated fraud, and make the Maryland system among the most vulnerable of all the states' new online voter registration systems. The purpose of this letter is to inform you of these risks and to recommend defensive steps for immediate implementation, as well as additional safeguards—described in an attachment to this letter—for implementation as soon as possible after the election.

Given the grave potential for harm, we urge the State of Maryland to take immediate defensive steps to safeguard the online voter registration system or else shut down the system. In either event, all transactions made so far should be carefully scrutinized for any signs that they were fraudulently submitted. While it is dangerous to make major changes in a voting system this close to an election without allowing sufficient time for careful development and testing by qualified experts, there are several short-term remedies and procedural changes that will reduce the risk of attack:

- *Record a complete transaction log for each completed or attempted online voter registration submission*, including the IP address of the computer submitting the request, and analyze transaction log data frequently for unusual patterns of activity that may indicate attempted fraud.
- *Regularly run exception reports which alert election officials about suspicious activity.* A severe "red flag" event would be a transaction attempting to use a drivers license number that *does not* match the MVA database but *would* be the correct number derived from the voter's name and birthdate if an MVA record did exist.
- *Require solving a CAPTCHA before each online voter registration transaction,* in order to make automated attacks against the website more difficult.
- *Require voters who register online to show their Maryland Driver's License* the first time they vote in Maryland, as originally required by the Help America Vote Act for mailed-in voter registrations.
- *Compare signatures on absentee ballot requests* that involve online registration changes to the signatures on file at the MVA.
- *Amend polling place procedures to reliably identify, record, resolve, and track problems involving voter registration.* (See detailed recommendations below.)

The problem lies in the way the Maryland online voter registration system authenticates applications and registration changes. Maryland allows no-excuse absentee voting and does not check signatures on the absentee ballot request or on the absentee ballot itself. Therefore, the integrity of the voting process relies heavily on the online registration system to authenticate voters and to ensure that fraudulent applications are not accepted.

In particular, Maryland allows a first-time voter to register online by entering his or her name, address, and date of birth on a website. In lieu of signatures, voters must submit a Maryland Driver's License or Motor Vehicle Administration (MVA) ID number. Already registered voters making registration changes enter the same information. Criminals who obtain this information can submit fraudulent registration applications and change requests in the names of Maryland citizens; so it is necessary to ask, how publicly available is the information?

Voters' names, addresses, and dates of birth can be obtained directly from the Maryland State Board of Elections (SBE) or the local boards of election (LBE), which sell voter registration data (see http://www.elections.state.md.us/pdf/SBEAPPL.pdf). The online registration system also asks for an MVA number; however, Maryland MVA numbers are derived in a straightforward manner from the license holders' names and birth dates. The method of deriving MVA numbers from this information is known to the public, and at least one website offers to calculate Maryland MVA numbers from data entered on the site. (See http://www.highprogrammer.com/cgi-bin/uniqueid/dl_md.)

Therefore, using only information published by the Maryland SBE (as well as by many other sources), a criminal could fraudulently log in to the Maryland online voter registration system and impersonate virtually any Maryland voter.

The ability to fraudulently impersonate Maryland voters enables several kinds of attacks that could disrupt or undermine the integrity of elections. By selectively targeting specific voters for registration changes (for instance, voters identified by the voter registration list as being affiliated with a particular party), it would be possible to use computers to affect the outcome of an election by:

- *Submitting large-scale address changes to legitimate, but incorrect, addresses.* Many voters would not realize that their mailing addresses had been changed in time to correct the problem. In addition, someone at the "new" address might be able to illegally cast a ballot for the victimized voter.
- *Submitting "nuisance" address changes* that reregister voters at random address. In this case, most of the registration confirmation cards would be returned to the BoE as undeliverable. As a result, voters would likely have to show ID with proof of address at the polls. If they did not have IDs with them, they would have to vote by provisional ballots and produce the IDs to the LBE before the provisional ballot canvass, or their votes would not be counted. If they had IDs verifying their real addresses and claimed they had not made the registration changes, it is unclear what would happen.
- *Submitting out-of-jurisdiction address changes* that would move a voter off the rolls of the jurisdiction of the contest the perpetrator is trying to influence. The result would be the same as above if the registration confirmation card bounced back to the LBE. If the card did not bounce back, the voter would be considered to have legitimately moved and probably would be required to vote by provisional ballot in his or her true precinct. In this case, only the contests that would be on the ballot in the "new" precinct would be counted, disenfranchising the voter from specific contests. Or the voter could go to the "new" precinct and vote on all the contests there, but he or she would still be disenfranchised from specific contests in the true home precinct.
- *Overwhelming the LBEs with a large quantity of new and/or changed registrations* right before the registration deadline. This would not allow much time to resolve problems, especially if large quantities of registration confirmation cards had to go out, and lots of bouncing cards had to be processed. The

result might be chaos and long lines at the polling place as election judges tried to process all the provisional voters or voters required to show ID.

- *Registering unregistered eligible voters.* Many eligible voters are not currently registered to vote in Maryland. Unregistered eligible voters could be gleaned from other lists of publicly available information such as telephone directories, Facebook, or other sources and fraudulently registered without their knowledge. Votes could be submitted for them either in person or via absentee ballot. Combined with online delivery of absentee ballots, this could make large-scale attacks easier because the ballot could be delivered to an email address and would not have to be intercepted physically.

At the very least, attacks such as these could wreak havoc at the polls on Election Day. At worst, they could disenfranchise legitimate voters or enable fraud that could affect the outcome of elections. While the potential for some attacks like the ones mentioned above also exists in the traditional paper-based voter registration system, there are significant differences in the scale, cost, possibility of detection, and evidence available for prosecution offered by an online system:

- *Scale:* Paper registrations have to be submitted one by one. Online registrations could be submitted via high-volume automated attacks programmed to submit the information to the website. These attacks could be made difficult to distinguish from legitimate transactions. They could originate from anywhere in the world. We note that many nations and foreign entities have a vested interest in the outcomes of American elections.
- *Cost:* Paper transactions incur postage fees and manual processing labor that could make large-scale attacks costly, especially attacks originating overseas. Online transactions are nearly cost-free.
- *Likelihood of detection:* Election officials would quickly raise an eyebrow if they received large quantities of registration changes in envelopes mailed from Iran or China, but they might never know the origin of changes submitted online. With paper-based registration, the following forensic evidence, which does not exist with online voter registration, would be available for prosecution:
  - *Signature:* Paper submissions require the voter's signature, which can be compared with the signature on file with the MVA or SBE. Online registrations replace the signature with a number.
  - *Physical evidence:* Paper submissions have a postmark with a date/time/place where the crime was committed. They may share similarities with other mailed pieces that would link them to the same perpetrator and tip observant election officials that something is amiss. Fingerprints or saliva left on the stamp or envelope seal might be used to establish the identity of the perpetrator. Online transactions leave no physical evidence and may be impossible to trace back to the perpetrator.

We sincerely hope that you will quickly address the problems we have outlined. Please let us know if there is any way that we can be of assistance.

Sincerely,

Prof. J. Alex Halderman
The University of Michigan

Dr. David R. Jefferson
Lawrence Livermore National Laboratory

Dr. Barbara Simons
IBM Research (Retired);
Former President, ACM (Association for Computing Machinery)

J. Alex Halderman is an assistant professor of computer science and engineering at the University of Michigan. His research spans computer security and tech-centric public policy, including topics such as software security, data privacy, electronic voting, censorship resistance, and cybercrime, as well as technological aspects of intellectual property law and government regulation. A noted expert on electronic voting security, 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. He recently led a team from the University of Michigan that hacked into Washington D.C.'s proposed Internet voting system. In his spare time, he reprogrammed a touch-screen DRE voting machine to play Pac-Man. He holds a Ph.D. in computer science 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 directs research in supercomputing and cyber security.

Barbara Simons recently published *Broken Ballots: Will Your Vote Count?*, a book on voting machines co-authored with Douglas Jones. She was appointed by Sen. Harry Reid to the Board of Advisors of the U.S. Election Assistance Commission, and she was a member of the workshop, convened at the request of President Clinton, that produced a report on Internet Voting in 2001. She also co-authored the report that led to the cancellation of Department of Defense's Internet voting project (SERVE) because of security concerns. Simons co-chaired the ACM study of statewide databases of registered voters, and co-authored the League of Women Voters report on election auditing. She chairs the Board of Directors of Verified Voting. 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.

Cc: Gov. Martin O'Malley
Attorney General Douglas Gansler
Sen. Joan Carter-Conway, Chair, Education, Health, and Environmental Affairs Committee
Sen. Roy P. Dyson, Chair, EHEA Ethics and Election Law Subcommittee
Del. Sheila E. Hixson, Chair, Ways and Means Committee
Del. Jon S. Cardin, Chair, W&M Election Law Subcommittee
Linda H. Lamone, State Administrator of Elections
Ross Goldstein, Deputy State Administrator
Assistant Attorney General Jeffrey L. Darsie

SUGGESTED SAFEGUARDS AND BEST PRACTICES FOR ONLINE VOTER REGISTRATION SYSTEMS *(DRAFT)*

During the online registration process:

Require an additional piece of personal information to be submitted with each new or changed registration to authenticate the transaction. The information should be readily available to the voter and easily authenticated by the SBE, but not generally available to the public. The last four digits of the Social Security number might be an example, because it is already used to authenticate UOCAVA voters who register online.

Require the user to solve a CAPTCHA before each transaction, in order to make automated attacks more difficult. Some states use a CAPTCHA system that requires the registrant to type in a randomly generated string of letters or digits visually distorted in ways not easily read by machines.

Record a complete transaction log for each *attempted or completed* online voter registration submission, including:

- The IP address of the computer submitting the request;
- Timestamps and browser user agent string;
- Before and after data for changes (address, party, name, etc.).

Analyze transaction log data frequently for suspicious patterns of activity. Compare results with historical data and with other states for:

- Number of successful requests for new registrations;
- Number of unsuccessful new registration attempts and reasons for rejections;
- Number of requests for registration changes, sorted by type of change;
- Number of unsuccessful attempts to change and reasons for rejections, sorted by type of change.

Regularly run exception reports which alert election officials about:

- Changes or new submittals for drivers license numbers for which no matching record exists in the MVA database, especially those which would be the correct number derived from the voter's name and birthdate if an MVA record did exist. (The only likely cause for this event is attempted fraud).
- Many changes made at the same time, from the same IP address, or from the same region outside the state or overseas;
- Unusual numbers of changes affecting a specific voting district;
- Unusual party affiliation changes;
- Recurring addresses, phone numbers or e-mail addresses submitted.

Perform ongoing security testing throughout the active voter registration period, contracting with qualified cybersecurity experts to perform:

- Active intrusion detection and prevention;
- Frequent vulnerability assessments;
- Regular penetration testing.

For example, Nevada monitors error logs to identify hacking attempts. Colorado contracts with a cybersecurity firm and has found that bad actors are repeatedly trying to break into the state's computer systems.

Have a disaster recovery plan that allows transactions to be rolled back to the existing state before an attack if suspicious patterns are detected in individual or large-scale changes. Maintain the ability to:

- Roll back the database to a specific date and time;
- Undo changes for a specific type of transaction, such as change of party affiliation or change of address in a specific geographic area;
- Notify affected voters that their transactions are being reviewed and may need to be reverified.

Set the election schedule to allow ample time between the closing of online registration and the beginning of voting. The schedule should allow sufficient time for the state to mail out confirmations and for the voter to report any problems.

Mail confirmation of registration or changes to the voter, marked “return if undeliverable.”

- In the case of address changes, notifications should be sent to both the voters’ old and new addresses (as is currently done in Colorado).
- Inform voters that the change initiated online is not official until approved by the election office and confirmed by notification via US mail.

During the online process, the voter should be given a contact to reach if they do not receive a letter from the state within a specified period of time.

During the voting period:

Require voters who register online to show their Maryland Driver’s License the first time they vote in Maryland, as used to be required for mailed-in registrations (except UOCAVA voters, who are allowed to use Social Security numbers instead). Since online registrants, by definition, possess a driver’s license or MVA ID number, they should be required to show it the first time they vote to establish their identity.

Compare signatures on absentee ballot requests that involve online registration changes to the signatures on file at the MVA. Clear discrepancies in signature matching should initiate contact with the voter to verify the transaction before an absentee ballot is sent

Maintain procedures for identifying, recording, and resolving problems at the polling place.

- The provisional ballot code “Other Reason” should be used to identify those voters who claim that a change was made to their registration without their authorization, and who are therefore required to vote a provisional ballot.
- A provisional voter who claims an absentee ballot was submitted without their knowledge or consent should have the signatures checked on both the absentee and provisional ballots to determine if either signature appears to be fraudulent.
- A voter who was “moved” out of their home precinct through a fraudulent transaction should have their ballot counted fully as if it was cast in the correct precinct.
- Provisional and absentee voting data should be analyzed and compared to other jurisdictions and historical data to identify any anomalous voting patterns.