November 17, 2015

Statement to the Senate State Government Committee Re: SB 1052

Verified Voting is a national, non-partisan, not-for-profit organization committed to safeguarding democracy in the digital age. We advocate for voting technology and policies that promote and improve transparency, accessibility, security and auditability in the election process. We are writing today to express our opposition to Senate Bill 1052, a bill which would permit the return of ballots by electronic transmission over insecure Internet means for military voters in Pennsylvania, and to urge you to vote NO on SB 1052.

Ballots sent by email are vulnerable to undetectable manipulation or tampering while in transit over the Internet.[i] Ballots sent by fax are also vulnerable to attackers. Today most facsimiles are sent via Internet over facsimile mail programs which have the same threat profile as emailed ballots. By permitting the electronic return of voted ballots, SB 1052 will significantly damage the integrity of Pennsylvania's elections and put the ballots of military voters at grave risk.

Department of Defense and National Institute of Standards and Technology oppose online voting.

At the start of the 21st century the promise of secure Internet voting seemed attainable; Congress directed the Department of Defense (DOD) in the 2002 National Defense Authorization Act (NDAA) to develop an online voting system for military and overseas voters. The Federal Voting Assistance Program (FVAP), an agency administered by the DOD, developed a system for deployment in 2004. After a security review the DOD cancelled the project because it could not ensure the legitimacy of votes cast over the Internet. In 2005 Congress directed the National Institute of Standards and Technology (NIST) to study the online return of voted ballots for the purpose of setting security standards so DoD and FVAP could develop a secure online voting system for military voters. NIST published numerous reports on its research, and documented several security issues that cannot be mitigated or solved with the cyber security safeguards and voting system protocols currently available. NIST concluded that until these challenges are overcome, secure Internet voting is not yet feasible. [ii]

For these reasons the Department of Defense has warned that it cannot ensure the legitimacy of ballots sent over the Internet and has stated ***"[the Department of Defense] does not advocate for the electronic transmission of any voted ballot, whether it be by fax, email or via the Internet."***[iii] In addition, the Federal Voting Assistance Program, in a report to Congress in 2013, stated clearly that the postal mail return of a voted ballot, coupled with the electronic transmission of a blank ballot is the "most responsible"[iv] method of absentee voting for UOCAVA voters. The overwhelming evidence that secure Internet voting is not within our grasp led Congress to repeal, in the 2015 National Defense Authorization Act, the earlier directive that DoD pursue online voting for military and overseas voters.

It is not reasonable to expect the Pennsylvania Department of State should be able to develop a secure online ballot return system when the Department of Defense and the National Institute of Standards and Technology have determined secure online voting is not presently achievable.

Though a number of states currently allow some form of email or electronic ballot return, that does not mean that it is safe or secure. Most of those states passed bills to allow voted ballots to be returned over the Internet before the severity of today's online threats was fully matured, understood or recognized. In recent years national cyber security experts have sounded increasing urgent warnings that the Internet is

highly insecure, impossible to safeguard absolutely, rich with possible avenues of attack and rife with potential attackers. Security experts have warned repeatedly that the ability of hackers to infiltrate a system has advanced much more rapidly than the security tools used to resist them. Internet systems have become less secure and more susceptible to attack over the last ten years.

As director of national intelligence James Clapper testified to the U.S. Senate Intelligence Committee, "*...cyber intruders have found more ways to get around detection and attribution technologies. Both state and non-state actors* ***have grown more sophisticated in their capabilities to circumvent cyberdefenses.***"[v] [Emphasis added.]

Opposition to Internet voting.

The National Institute of Standards and Technology and the DOD are not alone in concluding that online voting cannot be done securely. Experts at the Department of Homeland Security[vi] have warned that online voting is not advisable. Computer science experts in the private sector have joined in strong opposition to the implementation of online voting.[vii] U.S. Vote Foundation (formerly the Overseas Vote Foundation) spent over two years researching secure online voting. The resulting report, published this past summer, found that the problem of securing an online election cannot be met with the security tools currently available.[viii] Utah's Lt. Governor Spencer Cox, a proponent of online voting, convened an advisory group to provide guidance for the state to expand online voting. However, after a year of study, the Lt. Governor's own advisory group concluded that online voting cannot currently be done securely and states the problem of secure online voting in clear terms:

> "*Given that sufficiently secure Internet voting systems do not yet exist, they would need to be built. Of course, some systems, like a stone bridge to the moon, are impossible to build. Others, like a stone bridge to Hawaii, are so exorbitantly expensive as to remain a fool's errand. However, other systems, like spacecraft, aircraft, and the newer Sam White Bridge, are much more affordable. Unfortunately, with the four challenges mentioned in the preceding section, the unconstrained nirvana of Internet voting, "from any device, entirely online," is so impossible, or at least infeasible, as to be a fool's errand."*[ix]

Common Cause agrees, **"*today's email and Internet voting systems -- and those that will be available in the foreseeable future -- cannot be relied on to produce accurate, verifiable vote counts*."**[x]

The Heritage Foundation concludes, "[**t**]***hose who believe that it is "possible given current technology" to create a secure online voting system are dangerously mistaken…Internet voting, or even the delivery by e-mail of voted ballots from registered voters, would be vulnerable to a variety of well-known cyber-attacks, any of which could be catastrophic****."*[xi]

Online voting is not like online banking – it's much harder.

The public may ask, 'if I can bank online, why can't I vote online?' But voting includes some critical differences that make it a much more difficult enterprise than online banking or commerce. Online banking or shopping are neither secret nor anonymous; a customer can check her statement at any point to detect and address fraudulent charges. In Pennsylvania the secrecy of voting is protected by the Constitution, and no method may be put forward which fails to preserve that secrecy. Since the secrecy of votes cast online cannot be safeguarded, this alone should be cause to reject such methods. Further, the preservation of anonymity makes voting transactions more difficult to audit than banking transactions. There is no mechanism for the voter or election official to check to ensure ballots were not manipulated or hacked in transit and that the votes are legitimate. This makes online elections especially vulnerable to

undetectable hacking. Even if an attack were detected, there would be no way for election officials to determine which ballots were manipulated and which are legitimate, making an online attack uncorrectable.

Banks calculate an acceptable level of fraud and factor that into the cost of doing business or take out insurance to cover their losses. We can't do this with voting; we can't be willing to accept 2 or 3% of falsified ballots. Finally, the assumption that online banking can be done *securely* is faulty. It is estimated that banks lose millions or even billions of dollars every year to online attacks. High profile hacks like that on Citibank, JP Morgan Chase and Bank of America prove that even systems with high security budgets (much higher than the Pennsylvania Department of State) cannot resist determined attackers.

Estonia

Supporters of online voting often cite Estonia as an example of secure online voting but there are some important caveats and differences to consider. First, Estonian citizens all possess a government issued ID card with a chip in it which can offer a higher level of online voter authentication than is possible in the U.S. But more importantly, the Estonian system cannot correctly be described as "secure" as computer security researchers have identified vulnerabilities in the system that make it susceptible to manipulation and undetectable hacking.[xii] Finally, it is important to note that there is considerable public distrust of the system in Estonia. Many citizens contend that the online voting system has been manipulated by Russian operatives**.** Public confidence in our election process is essential. We should not be willing to accept a system that cannot be trusted to be legitimate.

In conclusion: we know much more today than we did five or ten years ago about the insecurity of systems on the Internet. Ten years ago secure Internet voting seemed an attainable goal but in 2015 experts have come the consensus that the secure online return of voted ballots is a much more difficult problem to solve and that the likelihood of a malicious attack is all too real. The mounting evidence that secure online voting is not yet achievable led the U.S. congress to abandon it as a project. Pennsylvania would be unwise to move to adopt a practice we now know cannot be secured. We urge the committee to vote NO on SB 1052.

---

[i] NIST IR 7551 "A Threat Analysis of UOCAVA Voting systems" http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf

[ii] http://www.nist.gov/itl/vote/uocava.cfm

[iii] Pentagon spokesman Lt. Commander Nathan Christensen, April 16, 2015

Gordon, Greg, "As states warm to online voting, experts warn of trouble ahead," The Olympian, April 16, 2015

iv Federal Voting Assistance Program, May 2013, "2010 Electronic Voting Support Wizard (EVSW) Technology Pilot Program Report to Congress http://www.fvap.gov/uploads/FVAP/Reports/evsw_report.pdf

[v] McCarter, Mickey, "Cyber Security Officials Warn of Advanced Cybersecurity Threat to US Agencies, Business," *Homeland Security Today,* Feb 2, 2012

[vi] Fessler, Pam, "Online Voting 'Premature,' Warns Government Cyber Security Expert," *National Public Radio,* Mar 29, 2012

[vii] "Computer Technologists' Statement on Internet Voting," https://www.verifiedvoting.org/projects/internet-voting-statement/

[viii] "The Future of Voting," U.S. Vote Foundation July 2015 https://www.usvotefoundation.org/e2e-viv/summary

[ix] "iVote Advisory Committee Final Report," Aug. 21, 2015

http://elections.utah.gov/Media/Default/Documents/Report/iVote%20Report%20Final.pdf

[x] "Online voting – Not so fast," Common Cause, http://www.commoncause.org/issues/voting-and-elections/registration-and-voting-systems/online-voting-not-so-fast.html

[xi] Spakovsky, Hans, "*The Dangers of Internet Voting,"* The Heritage Foundation, July 14, 2015

http://www.heritage.org/research/reports/2015/07/the-dangers-of-internet-voting

[xii] Security Analysis of the Estonian Internet Voting System, Drew Springal, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Maggie MacAlpine, J. Alex Haldermann. *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS '14), November 2014 https://estoniaevoting.org/findings/paper/