Testimony of Verified Voting
Contact: susan@verifiedvoting.org
917 796 8782
New York State Assembly
Standing Committee on Election Law
Subcommittee on Election Day Operations and
Vote Disenfranchisement

Re: Election Integrity
November 27, 2017

Thank you for the opportunity to testify on election system security in today's cyber threat environment.

Verified Voting is a national non-partisan, not for profit research and advocacy organization committed to safeguarding democracy in the digital age. Founded by computer scientists, Verified Voting's mission is to advocate for the responsible use of emerging technologies to ensure that Americans can be confident their votes will be cast as intended and counted as cast. We promote policies that provide for auditable, accessible and resilient voting for all eligible citizens. We commend the Committee for its attention to this critical issue.

In 2016 the threat of cyber attacks on our elections from foreign entities became an alarming reality. We learned that an adversarial nation was targeting our election systems with the intent to disrupt and undermine the legitimacy of our free, democratic government. In the declassified report "Assessing Russian Activities and Intentions in Recent U.S. Elections" the U.S. Intelligence Community warned that "Russian intelligence obtained and maintained access to elements of multiple US state or local electoral boards."[1] Several months ago we learned that the U.S. Department of Homeland Security (DHS) contacted officials in twenty-one states to notify them that their election systems had been targeted by Russian hackers. When asked at a June hearing of the Senate Select Committee of Intelligence if we should expect continued cyber attacks on our election infrastructure, then FBI director James Comey stated emphatically, "[t]hey will be back."[2] The gravity of this threat cannot be overstated. It is critical that we take every precaution to protect our election systems.

The stealth, skill and sophistication of today's state-level cyber attackers should not be underestimated. Cyber security experts have warned that attacks today continue to outpace our ability to defend against them. The unending list of high profile and well-defended enterprises that have fallen victim to cyber attacks[3] demonstrates the impracticality of trying to defend any computer system absolutely. Further complicating the problem, our election offices are typically under-resourced and understaffed. Though the New York State Board of Elections currently has

[1] https://www.dni.gov/files/documents/ICA_2017_01.pdf
[2] "Full Text: James Comey testimony transcript on Trump and Russia," *Politico,* June 8, 2017
[3] Center for Strategic and International Studies, "Significant Cyber Incidents" https://www.csis.org/programs/cybersecurity-and-warfare/technology-policy-program/other-projects-cybersecurity

in place some of the more advanced cyber security and cyber hygiene requirements for election systems, we cannot expect our county election offices to defend against cyber attacks from a state-level attacker.

Post-election audits are an essential election safeguard

Computer security experts have maintained that absolute cyber security is unattainable. Many have advocated that the best defense is to assume your system has already been hacked. We must accept that we can't have absolute security of any computerized system, including voting systems, but we can strive for *resilience* to cyber attack in computerized systems. A computer system resilient to cyber attack would still function properly even if it's been compromised. Resilience in an election system would ensure that even if an election system is attacked, voters would still be able to vote, have their votes counted correctly, and the election outcome would reflect the will of the people. In other words, a resilient election system could be hacked, but we could still have confidence that it will produce the correct election outcome.

We can achieve this resilience in elections by utilizing voter-marked paper ballots which provide a durable, physical record of voter intent that is out of reach of a cyber attack, and conducting robust post-election manual ballot audits designed to detect and correct possible errors in the election outcome. This can be attained with strong post-election manual ballot audits that have automatic escalation requirements and a legal mechanism to replace the computer generated result with the hand counted tally whenever the hand tally indicates that the electronic tally was incorrect.

A well-designed manual post-election audit ensures this resilience in the election process by providing a high level of statistical confidence that any potential error in the electronic vote count affecting the outcome of the election would be detected and the election outcome would be corrected by escalating the manual audit to a full hand count. In other words, even if a cyber attack successfully manipulated an election by changing the computerized vote tally, the manual audit would escalate to a full hand count of the paper ballots and amend the corrupted electronic election result.

Perhaps most importantly, post-election manual ballot audits should provide transparency in the election process, affording voters and candidates evidence that the election result is correct. This transparency in the election process will eliminate questions of "election rigging" and boost voter confidence.

A robust, manual post-election audit designed to correct an error in the computer generated election results must have several essential features: 1) The audit must be mandatory and routine, performed on all contests without requiring any action by election officials, candidates or the public to initiate it. 2) The audit must be designed to provide a high level of statistical confidence that the election outcome is correct. 3) The audit must be performed before certification of the election outcome so that a potential error can be detected and corrected before certification of the winners. 4) Errors detected by the audit must force an automatic escalation of the audit (again without requiring action by any party) to a full hand count if necessary. 5) The full hand count must supersede the computer-generated tally automatically. 6) The post-election manual ballot audit should be transparent to voters and all relevant documentation - including ballots audited, discrepancies found, escalation (if necessary), and audit results - should be publicly posted.

New York State currently requires post-election audits however, the New York State audit law falls short of many of the essential features described above. Current law requires a post-election audit of 3% which escalates if there are discrepancies. However the mechanism to escalate to a full hand count, which would supersede the computer generated count, is dependent on agreement of the bipartisan election board. As Common Cause has identified, it's to be expected that the election commissioner of the leading party would be unlikely to challenge that lead by pursuing a full hand count. Furthermore, NY's 3% flat audit rate does not provide a high level of statistical confidence that the election outcome is correct and county election officials are not required to publicly post details of the post-election audit. New York State election law also permits automated audits conducted by computers which can also be compromised by cyber attacks.

The short-comings of New York's current audit law can be resolved by adopting a "risk-limiting audit." A "risk-limiting audit" (RLA) is an audit of an election contest that provides strong statistical evidence that the election outcome is right. Importantly, a risk-limiting audit has automatic mechanism to escalate to a full hand count if necessary and provides a high probability of correcting a wrong outcome. If the margin of victory is very close a risk-limiting audit requires examining a larger sample of ballots to attain a high statistical confidence that the election outcome is correct. If the margin of victory is wide, fewer ballots need to be reviewed to ensure with high confidence that the outcome is correct—assuming that the audit does not uncover problems. In most cases, the 3% flat audit that is performed currently in New York State would greatly exceed the number of ballots hand counted for a risk-limiting audit, making risk-limiting audits more efficient and cost effective. Colorado recently conducted a successful state-wide risk-limiting audit on its November elections. New Mexico conducts similar audits and Rhode Island just passed legislation to require risk-limiting audits by 2020.

We urge the Assembly to consider amending New York State's post-election audit law to require New York State conduct risk-limiting audits. We welcome the opportunity to work with members on this critical election security safeguard.

<u>New York's recount/recanvas laws need updating</u>

Before transitioning to paper ballots and optical scanners, New York State residents voted for decades on mechanical lever machines. Lever machines do not produce a record of individual ballots or votes. Instead, they maintain a running tally on the mechanical counters limiting any recount to a review and re-tabulation of the totals taken from each lever machine, known as a recanvas. New York State recount or recanvas law has not been updated to reflect the ability to recount paper ballots should circumstances require. The law still refers to a recanvas which can be interpreted to merely re-tabulate the totals from each optical scanner. We encourage the Assembly to update the recount/recanvas law to specify that a recount should be conducted by manually counting the voter-marked paper ballots and would be happy to provide assistance on this topic.

<u>New York should eschew internet voting or any type of online ballot return</u>

We would like to discourage any consideration of Internet voting including email or facsimile return of voted ballots or through online ballot transmission systems. Decades of research has shown it is not possible to transmit ballots securely over the Internet. With today's threat of foreign cyber attacks on our elections, we must assume those systems would be the first target and recognize those ballots will be the easiest to manipulate.

Researchers for the federal government have spent a decade and a half and over 100 million dollars to study ways for the military to return ballots securely through online methods.[4] The Department of Defense has attempted pilot projects for online ballot return and concluded that it is currently not possible to ensure the security, privacy, auditability, integrity and legitimacy of ballots cast over the Internet.[5] For this reason, the U.S. Election Assistance Commission did not set security standards or guidelines for an Internet voting pilot project to be carried out by the Department of Defense (DoD) for military and overseas voters. There are no federal security guidelines because the federal government concluded online voting cannot be done securely.[6] Moreover, because federal researchers determined that secure online voting is not currently feasible, the DoD did not develop an online voting system for military voters. The conclusive evidence that online voting cannot yet be done securely led the federal government to abandon its effort to develop a secure online voting system for the military in 2014.[7]

The overwhelming evidence that secure Internet voting *still* is not within our grasp led Congress to repeal that directive to the Department of Defense to pursue online voting for military and overseas voters in the 2015 National Defense Authorization Act. The question of how to develop a secure online voting system has been asked and answered by researchers at the federal government. Secure online voting is not yet achievable. Vendors of electronic ballot return systems may claim that their systems are secure but these security claims are backed solely by the vendors' promises and are completely unsubstantiated. ***Any claim by a for-profit vendor that it has developed a secure ballot return system is in direct contradiction to the best assessment of federal researchers after years of research and analysis.***

For these reasons 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."***[8] In addition, the Department of Defense's Federal Voting Assistance Program, in a report to congress in 2013, stated that the postal mail return of a voted ballot, coupled with the electronic transmission of a blank ballot is the "most responsible"[9] method of absentee voting for military and overseas voters.

While it is true that 32 States do allow electronic ballot return for military and overseas voters it is important to understand that in most of these States the provisions to return ballots electronically were passed *before* federal researchers had conducted this research and reached these conclusions. New York has the benefit of this research conducted in the last decade. We need to make use of this research and heed the warnings that foreign actors are targeting our electoral systems. The events of the last election cycle should be driving the move *away* from online ballot return.

---

[4] Department of Defense Fiscal Year (FY) 2015 Budget Estimates March 2014, DoD Human Resources Activity *Defense Wide Justification Book Volume 5 of 5 Research, Development, Test & Evaluation, Defense-Wide*

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

[6] GAO report 10-476 Elections, "DOD Can Strengthen Evaluation of its Absentee Voting Assistance Program." June 2010

[7] In the Carl Levin and Howard P. "Buck" McKeon National Defense Authorization Act for Fiscal Year 2015 (Public Law 113-291) congress repealed a directive initiated in 2002 to the Department of Defense directing it to develop an Internet voting demonstration project for military and overseas voters.

[8] 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

[9] 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

Thank you very much. We greatly appreciate the opportunity to provide testimony today and we welcome the opportunity to work with the committee and members on these issues. Please feel free to contact me if I can be of any assistance or provide any additional information or research.