40 NORTH PEARL STREET, SUITE 5
ALBANY, N.Y. 12207-2109

Douglas A. Kellner
Co-Chair

STATEMENT FOR THE ELECTION ASSISTANCE COMMISSION

DOUGLAS A. KELLNER
Co-Chair, New York State Board of Elections
April 18, 2018

New York Governor Andrew M Cuomo made election security a priority issue in his State of the State message in January of this year. The Legislature recently helped the Governor to deliver on that priority by enacting his budget proposals, which included substantial funding for improving the security of our election infrastructure, and by requiring disclosure of internet advertising designed to influence election outcomes. amidst reports of Russian interference in the U.S. 2016 election.

Governor Cuomo established the New York State Cyber Security Advisory Board to work with State agencies and the State and County Boards of Election to assess the threats to the cyber security of New York's elections infrastructure, identify security priorities, and recommend any necessary additional security measures. To date, there have been no credible reports of electoral system disruptions in New York. Nevertheless, Governor Cuomo correctly noted that, "The integrity of the electoral system is essential to a functioning democracy, and with those core American principles under attack, we must take decisive action to safeguard democratic integrity and expand voting rights." He noted that, "In New York, we have taken aggressive action to reform our electoral system and restore people's trust in government. Recent reports of foreign hacking on the American electoral system are highly disturbing, and New York will do everything in its power to continue to secure our electoral system and protect the sanctity of our elections. In the absence of a concerted federal response, New York State is stepping up to ensure we are prepared for the serious cyber threats facing our electoral system."

Governor Cuomo created the Cyber Security Advisory Board to ensure the State maintains a cutting-edge strategy to keep New Yorkers safe from cyber threats. The Board is comprised of world-renowned cyber security experts who advise the administration and make recommendations for protecting the state's critical infrastructure and information systems.

These actions are only the latest in an extensive number of steps undertaken by New York State since reports of potential Russian interference began to surface prior to the 2016 election. Through a partnership between the Executive Branch, the State Board of Elections, the New York State Association of Counties, and the Federal Bureau of Investigation, the State Intelligence Center worked closely with the State and County Boards of Elections to protect their systems and develop secure voting website backup plans. These included a comprehensive security review of the DMV's Electronic Voter Registration system, scanning the State Board of Elections systems for potential vulnerabilities, and advanced monitoring of network traffic and system logs at the State Board of Elections.

The NYS Intelligence Center established a 24-hour call center where counties could report and receive assistance for potential disruptions, supported by secure communications channels that connected New York with resources from federal agencies and other states. Additionally, weekly briefings were held throughout the election cycle to monitor threats and further coordination among partners.

The FY 2019 Budget adopted on March 31 includes $5 million to implement a four-pronged strategy to further strengthen cyber protections for New York's election infrastructure: create an Election Support Center, develop an Election Cyber Security Toolkit, provide cyber risk vulnerability assessments for State and County Boards of Elections, and require County Boards of Elections to report data breaches to State authorities.

Disclosure of paid internet advertisements

I believe that New York is the first state to require disclosure of paid internet advertising that are political communications designed to affect the outcome of elections (although the City of Seattle has required disclosure of internet advertising for several years.

One interesting feature of the new law is the requirement that the New York State Board of Elections "maintain and make available for public inspection in a machine readable format, a complete record of any independent expenditure in the form of paid internet or digital advertisement required to be filed." The State Board of Elections is now examining how it will implement this mandate as we draft regulations. I have raised the question that if the board of elections starts posting video advertisements, will our web site evolve into a new version of You Tube for the New York political market.

Voting System Security

New York created the gold standing for voting system security when it enacted the Election Modernization and Reform Act of 2005 in order to bring New York into compliance with the Help America Vote Act. New York's law has gone far beyond the federal requirements for securing the voting system from external threats. Key features of the New York safeguards are:

- Requirement for a voter verifiable paper audit trail;

- When scanners are used, the scanner must make a randomized record of each ballot image and its associated cast vote record;

- No voting equipment can be capable of connecting to the internet or any other form of wireless communication;

- There is a robust certification process (indeed flaws in the federal certification process led the EAC to suspend the accreditation of its test lab in 2008 and to completely overhaul its certification testing system;

- New York's certification process includes review of the voting system source code, and escrow of the certified source code;

- Counties may use only copies of the certified source code that are physically delivered to them by the State Board;

- The computers a county board uses for its election management system may not be connected to the internet and can use only software approved and escrowed by the State Board;

- Only election officials are allowed to program the ballot setup; counties are prohibited from contracting out this process to vendors;

- There is a post-election audit of three per cent of the voting machines in each county.

This year a number of counties will begin using automated tools to make the audit process more efficient and more accurate. We recently authorized the system and procedures proposed by Clear Ballot for use in New York. These include rescanning the voted ballots into off-the-shelf scanners using Clear Ballot software that is completely independent of the software used for the voting system scanners. In addition, the process for using the automated tool requires a manual comparison of specified amounts of randomly selected ballots to assure that the Clear Ballot system has accurately recorded the votes on these ballots**.**

EAC VVSG and Certification Implementation

I recognize that the federal Voting System Guidelines are "Voluntary." Nevertheless, the EAC should exercise guidance to the states on minimal *sine qua non* requirements. If a voting system is not accurate, transparent and verifiable, it should not be used—period. The VVSG should unambiguously require a voter verifiable paper audit trail. States that do not meet this minimal standard should be urged to upgrade their voting systems.

The VVSG include a number of provisions that say a voting system "should" have a particular feature. Although these "shoulds" are not mandatory, when the EAC issues a

certification report, the report should unambiguously identify each feature of the voting system that does not comply with a "should" in the guidelines. The report should be written with non-technical language that allows election administrators to understand the shortcomings in any system they are considering to acquire.

Internet and Blockchain

The EAC is very well familiarized with the numerous reports that show the substantial risks of internet voting. That is why New York law since 2005 has prohibited any voting equipment from having internet or wireless capability.

Recently, several proposals to use blockchain have circulated as way to have secure internet voting. While I want to encourage the exploration of new technology and methods to make voting more accessible and easier for our citizens, we also need to take a hard look before accepting innovative proposals at face value. I wish to credit Rebecca Wilson of SAVE our Votes in Maryland for organizing experts to provide this analysis of blockchains for voting.

Blockchain-based technology was developed for transactions with financial value, such as the cryptocurrency Bitcoin. It works by enabling an "authenticated public ledger" of "transaction" where the transactions are public but the identities of the people making them are disguised. The ledger is maintained on all of the computers of the people in the chain, working together as peers, with no centralized authority.

By contrast, elections are almost the opposite: they require a public ledger where the identities of the people (voters) making the transactions (voting) are known but the transactions themselves are hidden (secret ballot). Elections require a central authority to ensure that every legitimate person who is qualified to vote in the election and who follows the rules of the election (casting votes in the manner and timelines prescribed by law) has an equal voice in the outcome of the election.

If a blockchain functions correctly, (a) anyone with the correct software tools can check that transactions in the ledger were not manipulated after publication and (b) the failure or compromise of a single computer would not affect the functioning or integrity of the system. This has motivated many to propose that this technology solves the problem of secure voting over the internet.

In fact this technology does not solve any of the existing challenges in the design of secure voting systems. Most importantly, it introduces serious new problems of its own.

(1) The distributed agreement process used in blockchains creates a serious new liability for the voting process. Because blockchains do not have a centralized authority to ensure that all laws and rules of the election are being enforced equally and fairly, an entity that controls a majority of the computing resources used to construct a blockchain can arbitrarily change the contents of the blockchain, and even a large minority is sufficient to compromise its integrity.

Thus, use of blockchains for voting replaces rule by majority of voters with rule by whoever has the most computing resources. The more "powerful" computers in the blockchain could collude to misrepresent the entire list of transactions. The means that colluding computers (whether run by voters or foreign "bots") could selectively disenfrances smaller blocks of voters at will.

(2) Blockchains do no protect against all manipulation. A virus on the voter's computer could change her vote. Blockchains only enable the detection of manipulation *after* the transaction leaves the computer of origin (the voter's computer). No features exist for the user to easily detect manipulation by her computer. Much cryptocurrency theft occurs because a virus in the user's computer changes her transaction—and there is an underground industry in the development of such viruses. In effect, there is no way for the voter to verify that the voting transaction was recorded in the intended manner.

(3) We cannot know whether reported manipulations of the vote by the voter's computer are truthful. The cryptographic techniques used to detect manipulation in blockchains have been around for decades. End-to-end-verifiable (E2E-V) voting approaches enable alert voters to detect if their votes were changed by their own computers. However, we still do not know how to determine whether voters are being honest when they report such problems rather than casting doubt on the election outcome.

There are many other unsolved problems in internet voting that blockchains do nothing to solve. For example, blockchains do not prevent voter's credentials from being stolen—from email or other account hacks, phishing or spoofing attacks, hacked computers—and are as vulnerable to this problem as any other approach to remote electronic voting. Cisco recently detected a Ukrainian group named Coinholder which had stolen over $50 million in cryptocurrency by posing as blockchain exchanges. There a numerous other reports of similar schemes.