Larry Rockefeller
40 West 20th Street, Room 1100
New York, NY 10011

January 23, 2006

VIA HAND DELIVERY TO:

New York State Board of Elections
40 Steuben Street
Albany, NY 12207
Attention: Patricia Murray, Deputy General Counsel
Lee Daghlian, Public Affairs Officer

Re: Comments to Proposed Voting Systems Standards – Proposed Part 6209 of Subtitle V of Title 9 of the Official Compilation of Codes, Rules and Regulations of the State of New York

To the New York State Board of Elections:

Please accept the following comments on the voting systems standards ("the regulations") that the New York State Board of Elections has proposed to, among other things, comply with the federal Help America Vote Act of 2002, 42 U.S.C. § 15481 *et seq.* ("HAVA"), and the related enabling legislation enacted by New York, the Election Reform and Modernization Act of 2005.[1]

I. Introduction

I am a New York State voter with a long-standing interest in voting rights. I submit these comments because the regulations, if adopted, will unconstitutionally and illegally impair New Yorkers' fundamental right to vote.

First, the regulations place our State at substantial risk of electoral fraud. That is because the regulations implement new electronic voting systems for use in New York without adequate safeguards. These new technologies are rife with vulnerabilities and have presented serious security problems in past elections, as documented below. If these technologies are not properly regulated, a single ill-intentioned insider has the power to change the outcome of an election without being detected. These profound security problems have been recognized by respected authorities, including in reports by the non-partisan Government Accountability Office (GAO) (Exhibit A); by the bi-partisan Carter-Baker Commission (Exhibit B); and by the nation's leading computer

[1] Election Reform and Modernization Act of 2005, N.Y. Senate 5877, Chapter 181, 228th Legis. Session (as enacted Jul. 12, 2005).

security experts who, funded by the National Science Foundation, formed ACCURATE (Exhibit E).[2]

The proposed regulations overlook these security problems, and so expose New York elections to great danger of insider fraud. As noted in the enclosed affidavit of Dr. Douglas Jones, a leading expert on voting technology, the portion of the regulations "which provides for security requirements and provisions of the software, is **vastly inadequate**." Ex. W at ¶ 52 (emphasis added). His affidavit identifies more than 50 serious security flaws and other errors and omissions in the proposed standards that "put the voting rights of the citizens of New York at significant risk." *Id.* at ¶ 69. Because the regulations leave future New York elections open to manipulation and fraud, they must be withdrawn and revised extensively along the lines set forth in Dr. Jones's affidavit and below.

Second, the rush to implement the regulations guarantees chaos in the upcoming 2006 elections. Even if the regulations were ready to take effect, the Board's proposed course of action would still be fatally flawed. There simply is not enough time to implement new voting technology for elections later this year. In just the next few months, competing manufacturers' voting equipment must be certified, each of New York's 62 counties must select and purchase voting equipment, technical manuals must be written and distributed, election personnel be trained, and voting machines delivered, installed and tested. As explained below, when Florida attempted a similar task on a compressed timetable in 2002, complete electoral chaos resulted. County election officials in New York are "terrified" that the same thing will happen here,[3] and rightly so.

The solution is simple: maintain the status quo by keeping our existing lever machines in place while the security and other issues set forth herein are resolved expeditiously but carefully. To that end, the proposed regulations should be revised and the State should seek a waiver from the Department of Justice, like that sought by Connecticut, which will allow existing voting systems to remain in place for the 2006 elections. Doing so will allow New York adequate time to revise the regulations and then implement a rigorous certification, procurement and poll worker training process. The alternative of an unseemly rush to implement inadequate standards will infringe New Yorkers' right to vote. That intrusion on a fundamental constitutional right cannot be countenanced and could well result in voters taking expedited legal action to protect the right to vote. *See, e.g., Rockefeller v. Powers*, 917 F. Supp. 155 (E.D.N.Y. 1996), *aff'd* 78 F.3d 44 (2d Cir. 1996) (overturning state election practice as contrary to right to vote).

---

[2] ACCURATE is a multi-institution, interdisciplinary, academic research project funded by the NSF's "CyberTrust Program." Its principal investigators are associated with Johns Hopkins, Rice and Stanford Universities; the Universities of California and Iowa; and SRI International. Dr. Jones, whose affidavit is enclosed as Exhibit W, is one of the principal investigators. The ACCURATE Comment appended as Exhibit E is incorporated by reference as if fully set forth herein, as are all the other exhibits.

[3] *See* "Counties scramble to modernize voting machines," *The Journal News* (White Plains, NY: Jan. 8, 2006) (quoting a Rockland County commissioner of elections).

II. Background

As James A. Baker III and President Carter warned in their National Election Commission Report, the risk of insider fraud with respect to electronic voting machines is real:

> The greater threat to most systems comes not from external hackers, but from insiders who have direct access to the machines. Software can be modified maliciously before being installed into individual voting machines. There is no reason to trust insiders in the election industry any more than in other industries, such as gambling, where sophisticated insider fraud has occurred despite extraordinary measures to prevent it.

Ex. B at 28. These concerns are shared by all the major independent authorities who have considered election security, including the GAO, Ex. A at 25-26; the National Academy of Science's Committee on a Framework for Understanding Electronic Voting, co-chaired by former Governors Richard Celeste and Dick Thornburgh ("Governors' Report"), Ex. Z at ES-4 through ES-5; and ACCURATE, Ex. E at 10-17.

The potential to rig elections is far greater than in the old days of attempted ballot-box stuffing. Today's computer-based technology can allow a few individuals, or even one person, to practice fraud on a much larger scale, and to do so quickly and undetectably. *See* Ex. A (GAO Report) at 25-31; Ex. Z (Governors' Report) at ES-4 to ES-5. For example, memory cards used in the computers may easily be hacked, as demonstrated by a recent test in Florida showing how votes cast for one candidate could be switched to another. *See* Ex. F. To take another example, computer-based vote tabulators are programmed, serviced and, in certain circumstances, operated by technicians from private companies which, if partisan, creates additional risk. In the Ohio 2004 presidential election recount, a private election company with ties to one of the major political parties was alleged to have manipulated vote tabulation. Ex. J; *see also* Ex. I. These allegations, which are the subject of litigation, are extremely serious: a shift of just eleven votes per precinct from one candidate to the other would have changed the outcome of the election in Ohio. *See* Ex. K.[4]

These dangers are exacerbated by serious flaws in federal standards currently in place which are relied upon by the Board's proposed regulations. Those standards are minimal, weak and outdated. *See* Ex. E (Accurate Report) at 34-35. The next federal standards will not be ready until 2008. "The result of this timeline is that the majority of the systems in use will be certified to 2002 or 1990 standards....By allowing the use of

[4] Both of the foregoing examples concern optical scanning systems. In addition, four major studies by leading computer security experts have documented the failures of current "DRE" (direct recording electronic, i.e. "touchscreen") systems that were previously certified. *See* Ex. E at 10, n.24. For instance, researchers at Johns Hopkins University have also reported that weaknesses in a popular DRE security system could allow voters to cast multiple ballots without a trace. *See* Ex. G at 10. Studies commissioned by the State of Maryland concluded that, though security risks such as those detailed in the Johns Hopkins report might be fixable, no state or federal guidelines articulate requirements that reflect the unique demands of current electronic systems. *See* Ex. H.

systems certified to outdated standards, our voting system remains vulnerable. Errors and data corruption [are] introduced by delay...." *Id.* at 35.[5]

Moreover, enforcement of the federal standards is lax. Purported "Independent Testing Authorities" ("ITAs") are supposed to verify that electronic voting systems conform to the federal standards. But these ITAs are anything but independent, for they are paid by the very voting machine manufacturers they are supposed to regulate, rather than by the government. This creates a serious conflict of interest. *See* Exs. E and L.

To all of this, the election industry replies, in essence, "just trust us." *See* Ex. M. But trust comes harder when privately-held companies decline to disclose their ownership and count our votes with proprietary software and "trade secret" source code which they withhold from public inspection and audit. *See* Ex. N.

Consider the top two companies, which in 2004 counted two-thirds of the votes cast for the U.S. President, Senators and Congressmen. One is Sequoia Voting Systems, now owned by Smartmatic, a company rooted in Caracas and run in part by foreign nationals; the other is Election Systems & Software, based in Omaha, Nebraska. *See* Exs. O-R. Sequoia's parent, Smartmatic, has had known ties to the Venezuelan government. It was at the center of a national controversy surrounding the recall election won by President Hugo Chavez in 2004, for which it provided the electronic voting systems. *See* Ex. S. However, because current U.S. election laws do not require Smartmatic to disclose the identity of any of its owners as a privately-held firm, there is no way for American voters to know who really controls the company.

Meanwhile, Election Systems & Software (ES&S) also does not reveal who owns it, despite its website's boast that "ES&S systems have counted approximately 56 percent of the U.S. national vote in each of the last four presidential and congressional elections, amounting to more than 100 million ballots cast in each election." Ex. R. That includes the presidential election of 2000, where ES&S supplied the punchcard ballots to Miami-Dade County and Sequoia supplied Palm Beach County. *See* Ex. T. The Board should investigate and consider these companies' histories and backgrounds with respect to punch-card voting, which cast light on whether they can be relied upon to provide DRE or optical scanning systems that are secure against insider fraud.[6]

---

[5] The outmoded standards are likely be to blame for many of the 57,000 voter complaints of irregularities in the 2004 presidential election. *See* Ex. E (ACCURATE Report) at 30-31.

[6] To inform the very issues now before New York relating to the reliability of the voting machine manufacturers, Assemblyman Keith Wright, the Chair of the New York Assembly election committee urged the Florida Secretary of State to preserve the unused paper ballots from 2000 (their chads still intact), so that a scientific examination could determine whether ballot paper flaws caused the high number of votes disqualified mostly in urban areas. *See* Exhibit Y, Letter from Keith Wright, Chair of the N.Y. State Assembly Committee on Election Law, to Florida Secretary of State Glenda Hood (Jun. 30, 2003). In response, the Florida Secretary of State defended in court her right to destroy the ballots. *See Rogers et al. v. Hood, et al.*, 906 So.2d 1220 (Fla. 1st DCA 2005). As a result, no satisfactory answer has ever been received from Florida. The Board should follow up and get to the bottom of this issue.

III. The Proposed Regulations Are Unlawful Because They Undermine Electoral Security and Order.

A. The United States and New York Constitutions and Laws Guarantee Voters the Right to Secure and Orderly Elections.

The United States Constitution guarantees the right of all citizens to have their votes counted in honest elections. *See Anderson v. United States*, 417 U.S. 211, 227 (1974); *see also Anderson v. Celebrezze*, 460 U.S. 780, 786-88 (1983) (right to choose among candidates is fundamental). Voting is "of the most fundamental significance under our constitutional structure." *Illinois State Bd. of Elections v. Socialist Workers Party*, 440 U.S. 173, 184 (1979). The United States Supreme Court has declared that the right to vote freely for the candidate of one's choice is "the essence of a democratic society, and any restrictions on that right strike at the heart of representative government." *Reynolds v. Sims*, 377 U.S. 533, 555 (1964).

As a practical matter, states must regulate elections "if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic processes." *Storer v. Brown*, 415 U.S. 724, 730 (1974). Regulations "that protect the integrity and reliability of the electoral process itself," pass Constitutional muster. *Anderson*, 460 U.S. at 788 n.9. Conversely, state action that undermines the integrity and reliability of elections or otherwise burdens the right to vote will not stand. *See, e.g., Rockefeller v. Powers,* 917 F. Supp. 155 (E.D.N.Y. 1996), *aff'd* 78 F.3d 44 (2d Cir. 1996) (affirming district court's finding that New York State's ballot requirements, taken together, placed a substantial burden on the right to vote).[7]

Consistent with these principles, Congress enacted HAVA to promote integrity and reliability in the electoral process. HAVA is intended to ensure that voting and election administration systems "afford each registered and eligible voter an equal opportunity to vote and have that vote counted." 42 U.S.C. § 15381(a)(3) (goals to be promoted by the Election Assistance Commission).

Accordingly, the Board must interpret HAVA and the corresponding state enabling legislation in a manner that minimizes the risk that eligible voters will be deprived of their right to vote as a result of administrative action or omission. Indeed, recent comments by the Board and other state officials acknowledge this understanding of HAVA's goals. For example, Peter Kosinski, the co-executive director of the Board of Elections ("BOE"), stated that "[o]ur obligation is to make sure that voting works in New York state and to insure the integrity of the system[.]" Ex. U.

Those acknowledged duties of the Board are reinforced by New York state administrative law. That body of law requires that regulations be created pursuant to legislative objectives. *See Med. Soc'y v. Serio*, 800 N.E.2d 728, 734-35 (N.Y. 2003). Regulations must also, of course, be the result of appropriate fact-finding, deliberation

[7] These comments will focus on federal constitutional law, but similar concerns exist under the New York State Constitution. N.Y. Const. art. II.

and analysis by the Board. *See* N.Y. State Admin. Proc. Act §§ 202, 202-a (2006). If regulations do not conform to these requirements, they will be struck down by the courts.

B. The Regulations Do Not Afford the Level of Election Security Mandated By Applicable Law.

The proposed regulations violate the right of New York voters to secure elections. That is because the regulations fail to address the threat of insider fraud, the most serious security problem associated with the use of electronic voting systems. *See* Ex. B (Carter-Baker Report) at 28; *see also* Ex. E (ACCURATE Report) at 10-17; Ex. A (GAO Report) at 25; and Ex. Z (Governors' Report) at ES-4 to ES-5. As Governors Celeste and Thornburgh note, "the use of computers for voting purposes enables small numbers of individuals to practice fraud on a much larger scale than has been the case with nonelectronic systems." Ex. Z at ES-4 to ES-5. Moreover, the Board's failure adequately to address insider fraud pervasively undermines New York's entire voting system. For, as the Governors' Report explains, failing to guard against insider fraud not only leaves electronic voting systems vulnerable to manipulation, but affects other critical areas of the electoral process which are supported by computer-based systems: voter registration lists, vote tabulation, and ballot definition. *See* Ex. Z (Governors' Report) at ES-3.

1. The Proposed Regulations Fail to Assure Independent Review of Source Code.

The most important security feature which the regulations lack to protect against insider fraud is the requirement that source code be available for inspection and review by independent computer security experts. *See* Ex. B at 29; Ex. E at 11. Source code transparency is crucial to ensure the trustworthiness of voting systems, ability to verify accuracy of election results and to provide a basis for public confidence in the integrity of the system. *See* Ex. A at 36; Ex. B at 28; Ex. E at 10-11; Ex. W at ¶ 47.

The expert review panel under the regulations should consist of truly independent experts in lieu of reliance solely upon the federal ITA's (or their state equivalent). As discussed in Section II above, ITA's are anything but independent, as they receive payment from vendors whose machines they inspect. *See* Exs. E and L; *see also* "Help Monroe shop for new voting machines," *Democrat & Chronicle* (Rochester, NY: Jan. 4, 2006).[8]

The panel of independent experts must, moreover, have full and unhindered access to the source code and all relevant material. This panel must produce a public report which states the experts' analysis, the justifications for their conclusions and clear and convincing evidence which supports their conclusion regarding the security of the system. *See* Ex. E at 11.

---

[8] Moreover, if ITAs or their equivalent are a part of revised regulations, the Board must at a minimum require that they are not paid or selected by vendors whose systems they tasked to test and that they not have ties to partisan groups. *See* Ex. E at 4.

By contrast, the process of insider examination of source code proposed by the regulations in Section 6209.6 is grossly inadequate. The use of insiders worsens rather than reduces the serious risks of fraud, including the potential for the insertion of malicious code. *See* Ex. B at 28. While vendors' proprietary interests in source codes are legitimate, that interest is not outweighed by, and can easily be reconciled with, the public interest in transparency. *See* Ex. B at 29; Ex. E at 12; Ex. W at ¶ 47.[9]

Transparency is vital because it promotes voter confidence in our democracy and because the alternative, "veil of secrecy" approach destroys that confidence. ACCURATE eloquently explains that

> The current certification process occurs behind ... closed doors, leaving the interested public with no information about the process and no basis to trust the integrity of voting systems. Certification reports that indicate only whether a system passed are inadequate. For example, four major studies by leading computer security experts documented the failures of current DRE systems that were previously certified. Failing to make certification results available to computer security experts and other members of the public contributes to both the misconception that certified voting systems are state-of-the-art, secure, accurate and fair and the belief that voting machines cannot be trusted. Voter confidence cannot be sustained by hiding problems from the voting public. This "veil of secrecy" encourages questions regarding tampering and errors.

Ex. E. at 10-11 (citations omitted).

2. The Regulations Lack Adequate Security Assessment and Testing.

The regulations also fail to outline other needed requirements for software security assessment. As Dr. Jones writes in his affidavit,

> Subparagraph 2(1)(n), which provides for security requirements and provisions of the software, is **vastly inadequate**. Vendors should be required to identify each potential point of attack on the voting system, the technical defenses that are in place to guard against attack at each such point, and the procedural safeguards that are assumed to be in place to prevent each such attack. Where cryptographic materials are used, they should be clearly documented, including a discussion of how the key management problem is solved.

Ex. W at ¶ 52 (emphasis added). Software security provisions must be detailed and specific in order to prevent broad interpretation that leads to inconsistent testing. *See* Ex. A at 32; Ex. E at 14-15.

The best way to identify points of attack is through robust security testing. Yet the

[9] Both the ACCURATE report and the Carter-Baker Commission report point to good solutions for reconciling these interests. While each method is slightly different, both involve the requirement that independent computer security experts sign non-disclosure agreements to protect the proprietary interests of the voting systems vendors. *See* Ex. E at 12 and Ex. B at 29.

regulations ignore security testing and merely require so-called "functionality tests." *See* Section 6209.6(1)(C). Functionality tests examine the voting machines to ensure they operate correctly in situations where they are used as planned, whereas security tests look to how the machines operate when *unanticipated* circumstances or like insider threats arise. *See* Ex. E at 13. The Board's exclusive reliance on functional testing of voting machines is misconceived: even accurate functionality does not measure true security. *See id.*

In fact, past reliance on functional testing has proven to be a serious problem. For example, reliance on functional testing for voting systems verified under the 1990 and 2002 federal standards – which remain the most current federal standards in use today – resulted in systems entering the field with "numerous security and integrity problems." *See* Ex. E at 13. Furthermore, "functional testing alone, without threat analysis, code review, architectural analysis and penetration testing, will result in fundamentally insecure systems." Ex. E at 14. Upon redrafting, there must be provisions built into the regulations which require the appropriate security tests.

In particular, penetration testing ought to be incorporated in the requirements to ensure a thorough system security analysis. *See* Ex. E at 17. Penetration testing involves the simulation of a malicious attack on the system, potentially using insider information, in order to perform a critical system evaluation. *Id.* Requiring penetration analysis is crucial, since election security is "a national security issue, where the machinery we use to cast votes for elected offices and referenda must be trusted to the same degree as critical military, medical and banking systems." *Id.*

With respect to optical scanning systems, the regulations suffer from another testing deficiency. As Dr. Jones points out, they do not provide for testing the sensor calibration on optical scanning ballot tabulators. *See* Ex. W at ¶ 58. Miscalibration results in valid marks not being counted as vote and in other problems (such as invalid marks being counted). That can occur through negligence or design – the latter possibility constituting a serious security breach that could be accomplished by an insider working on the tabulators.

The proposed regulations also lack any provision requiring threat assessments. When threat assessments are conducted, the burden of proof should lie with the vendors to prove that their voting product is safe.[10] *See* Ex. E at 15. First, requirements addressing the properties of the system, what threats it must withstand, and the required level of assurance, must be established by a group of independent experts. Second, the requirements must provide a comprehensive list of attacks that must be addressed by the system. Third, vendors must provide evidence that their system is secure. Fourth, all this evidence must be available to independent experts for review. *See* Ex. E at 15.

Furthermore, the potential use of uncertified code is a serious potential hole in security which the proposed regulations do not address. The routine use of uncertified

[10] For an example of what a threat assessment system which places the burden of proof on the vendor would look like, please refer to the ACCURATE report, Exhibit E, at page 15.

code has been found in many states which have audited the use of code in voting systems. *See* Ex. E at 16. New York should take additional steps to ensure the integrity of the voting code and provide for procedures which would protect its integrity as it is stored, distributed and loaded into the machines.[11] *See* Ex. E at 16.

In addition to the serious security concerns with source code, the proposed regulations also fail to address security issues involved with other types of software used in voting systems. It is vitally important that independent security experts review all software on voting machines, not just source code. *See* Ex. E at 16.

3. The Regulations Should Address Voting Company Ownership and Political Donations.

Upon reconsideration of the proposed regulations, New York has an opportunity to take the lead nationally in promoting transparency not only with respect to source code review, but also in other areas which are deeply troubling to voters. The State should, first, lift the veil of secrecy regarding the ownership of vendors, especially those which are "privately-held." Specifically, the State should require that the vendor disclose the individuals who own the company, whether through direct or indirect investment (as through another entity). The State should also require disclosure of any ownership share held by a foreign government.[12]

The State should, second, promote public confidence by requesting that election systems vendors, and their senior management, voluntarily abstain from making political contributions to candidates for whom votes would be recorded and counted by software or source code to be provided by the vendor. Voters must know that the companies providing elections systems and their executives do not have preferred candidates in the elections those companies and executives are helping to run. This request should apply also to any testing laboratory or similar designee of the State Board involved in the certification or qualification of vendor software, source code or hardware under the proposed regulations.[13]

---

[11] As ACCURATE suggests, there should be procedures for "installing onto machines to ensure a chain of custody for th[e] code." Ex. E at 16. Also, "[p]eriodic auditing of code running in voting machines and backend systems should be performed. In addition, backend vote-tallying should be executed on isolated machines that have never been used for other purposes." Ex. E at 16-17.

[12] Requiring disclosure of foreign ownership would, for example, allow Sequoia to answer troubling questions about the relationship of its parent company Smartmatic to the Venezuelan government and other foreign nationals. *See* Section II *supra.*

[13] Such transparency is important to restoring voter confidence following experiences such as that in the 2004 presidential election in Ohio, where the central counting tabulators for 46 of its 88 counties were provided and serviced by two companies led by political partisans. *See generally* Letter from U.S. Representative John Conyers, Jr., et al. to Ohio Secretary of State J. Kenneth Blackwell et al. (Dec. 13, 2004), available at http://www.buzzflash.com/alerts/04/12/ale04100.html. To the extent permitted by applicable law, this voluntary bar should be made mandatory.

4. The Regulations Are Also Deficient In Many Other Respects.

The regulations suffer from many other problems over and above the security issues outlined above and in the exhibits hereto. As Dr. Jones notes in his affidavit, many definitions in the proposed regulations are simply incorrect. Also, the testing requirements for voting systems will exhaust local resources unless they are modified. And assumptions the proposed rule makes about how voting systems will function have not been tested against how the systems actually work. For example, definition of those marks on a ballot will be counted as a vote do not match what the voting systems may actually read as a vote.

The proposed regulations are, furthermore, insufficient in establishing true accessibility for voters with disabilities, as Dr. Jones mentions and a number of other comments on the proposed regulations have noted. *See* Ex. W at ¶ 31, 40. Taking additional time to revise the regulations will allow the Board to address these accessibility issues, including considering promising new non-electronic accessibility solutions which work better for the disabled and are more secure. *See, e.g.,* "Vote-PAD rocks the disabled vote," *Wired News* (at http://www.wired.com/news/technology/0,70036-0.html?tw=wn_tophead_3). The right of the disabled to vote and have their vote counted is no less important than for all other voters.

The proposed regulations (and the Board's regulations generally) also fail adequately to address issues relating to voter registration. For example, the Board has no regulations to ensure that voter registration in New York is not subject to risks such as roll purges by insiders or attacks by hackers. This must be remedied.[14]

The process that produced the regulations also falls far short of what is required by applicable law. As Dr. Jones notes,

> voting system standards cannot be written in a vacuum. Those responsible for promulgating voting system standards require expertise in voting systems, computer systems, security, and human factors in order to understand what standards are necessary and appropriate.... **In my opinion, the proposed voting standards for New York that I reviewed were not the product of an expert advisory committee or other expert resource.** New York State has excellent resources available to it on voting systems; it should bring those resources to bear in order to make real world voting system standards of which the voters of New York can be proud.

Ex. W at ¶¶ 66-67 (emphasis added).[15] For this and other reasons, "the proposed

---

[14] The Association of Computing Machinery has used its expertise to study this area in depth, and its recommendations with respect thereto will be published in a report later this month. Allowing additional time for revision of the regulations will permit the Board to take the findings and recommendations of ACM into account.

[15] It also does not appear that the Board has considered *any* testimony from a *disinterested* expert on voting systems, *i.e.,* a non-partisan and independent witness having no ties to the election industry. That conclusion follows from the review of three of the four public hearings – all that are publicly available right

standards, as written, fail to sufficiently regulate the electoral process to provide the necessary degree of security, integrity and reliability" required by law. *See id.* at ¶ 14.

C. The Rush to Implement the Regulations Will Guarantee Chaos in the 2006 Election.

In just over seven months, New York will hold vitally important primary elections for governor and for state and federal officers, including for the U.S. Senate and House of Representatives. As the experience of Florida in attempting a similar expedited process in 2002 teaches, that is not nearly enough time to get new voting technologies up and running. A rushed process will result in confused and dysfunctional 2006 elections, guaranteeing that many New Yorkers will be denied the right to vote. As explained below, the only rational course at this late date is to continue with the lever voting machines now in place, as the alternative is widespread deprivation of the franchise.

Consider all that must happen before the primary elections in September:

- The Board has yet to propose legally adequate regulations. Additional fact-finding will be required, including additional witness testimony. Then the regulations must be rewritten, published for comment, and only after the comment period ends, take effect. The comment period is generally at least 45 days long. Further, portions of the regulations may need to be addressed by the courts.

- Once final regulations are in effect, the state must certify offerings from the various voting machine manufacturers. Application forms (including highly technical data requests) must be created and completed by manufacturers. *See* Section 6209.4. Competing voting systems must then be physically delivered to the Board and examined, including testing, auditing and laboratory analysis. *See* Sections 6209.5-6209.6.

- Next, each of the 62 counties in the state must embark upon a procurement review to choose which voting system(s) they will use. *See* Section 6209.9. Should they use optical scan machines or DREs? Which manufacturer do they trust to help them safeguard votes and information? Which system will translate into actual accessibility for voters with disabilities? Manufacturers must be heard from, bids considered, and contracts negotiated. *Id.*

- Then the counties must train their boards of election personnel for the first time in the new technology and its use. This includes training for assembling

---

now – and the witness list for the fourth hearing. (The witness lists for all four hearings are attached as Exhibit X.) Absent such testimony, or other like evidence, the Board cannot fairly analyze the potential impact the rules may have on the electoral process. Moreover, because the Board apparently intends to finalize these regulations next month, it cannot possibly have the time to consider the thousands of pages of public comments (such as this letter and its attachments) and other information submitted. For the Board to fulfill its duties, it must consider truly independent evidence under a timetable that allows for meaningful review and analysis.

the machines, maintenance, storage, transportation, inspection, ballot layout and programming, as well as obtaining and distributing operations manuals for these and other activities. *See* Section 6209.9(A)(1)-(2). Each of these activities must then actually be undertaken by the newly-trained personnel to prepare for the election. Polling sites must also be surveyed and, if unsuitable for the new technology, remediated. *See* Section 6209.9(A)(3).

- Not only county election professionals, but also poll workers must be trained to assist voters with machines and malfunctions on election day. The Carter-Baker report notes that poll workers are poorly trained even now, although the systems they use are much simpler and easier to understand. *See* Ex. B at 50, 54-55. To implement DREs, poll workers will have to learn a great deal of complicated information and experience suggests they will have difficulty assimilating it, particularly the first time it is done and particularly if it is done in a hurry. *See* Ex. B at 25 n.64. The average poll worker's age is above 70, which means that many have little or no familiarity with computers or similar technology. *See* Ex. B at 54.

- Prior to the election, each County board must also conduct an acceptance test of each unit under the supervision of the State Board and certify the results to the State Board. If problems with the equipment are discovered, they must be corrected by the vendor. *See* Section 6209.10. Vendors can provide machines as late as 30 days before the election, and have up to 30 days to correct problems, so replacement machines may be delivered to some counties on the day before, the day of, or even the day *after* an election. *See* Section 6209.9(4)(a)(30 day pre-election delivery deadline); Section 6209.10(D) (30-day correction period afforded manufacturers).

- If the problems are serious, certification may need to be rescinded, which in turn requires notice and a hearing for interested parties. *See* Section 6209.8. Given the 30-day pre-election deadline for delivery of machines, if serious problems are discovered with a product, counties using it may be confronted with rescission on the eve of an election.[16]

It simply is not possible for all of the above to be done in the next seven months, and it certainly cannot be done right. County elections officials across the state recognize that. "I have to say I am terrified," Rockland's Commissioner of Elections said when asked about implementing the changes necessary to comply with HAVA.[17] Others have similar fears: "Even if the machines were delivered before the elections, the process is being rushed so much that some people fear an Election Day disaster: untrained

[16] The issues relating to timing that are set forth in this and the previous bullet point are serious flaws in the regulations that should be considered and remedied by the Board. Those flaws in the regulations are exacerbated as applied to the compressed schedule the Board is proposing prior to this year's elections.
[17] *See* "Counties scramble to modernize voting machines," *The Journal News* (White Plains, NY: Jan. 8, 2006).

inspectors and confused voters."[18] This sentiment was echoed by a Putnam Commissioner of Elections, who noted that "[t]he timetable just isn't there" as he explained that there would not be enough time to train inspectors or teach the public how to use new systems even if new machines are delivered this summer.[19] It is not far-fetched, then for voters to imagine "showing up to vote on Election Day and finding an unfamiliar voting machine and election workers who don't know how to operate it." *Id.*

Dr. Jones concurs that it would be a serious mistake for New York to rush to implement complex new voting technologies in the few months available before the 2006 primary:

> When states are pushed into adopting new voting systems within a short period of time, **it is a recipe for disaster. I strongly recommend that no jurisdiction put a new voting system into service at such a time that its first use is in a major election.** When a new voting system is put in place for the first time in a general election, any mistake will have serious national consequences. Based on my extensive survey of and experience with such matters, requiring adoption of new voting systems within a short period of time leads to chaos. The problems in Montgomery County, Pennsylvania in November 1996 and in Miami-Dade County, Florida, in their August 2002 primary are good examples of what can happen if a county pushes for rapid introduction of new voting equipment with its first use in a major election. In both cases, a county acted in haste to put a new voting system in place on an accelerated timetable, and the result was, in one case, a major lawsuit, and in the other, a national outcry. Ideally, the first uses of new systems should be in low-turnout elections where the impact of the problems, if any, will be minimal.

Ex. W. at ¶ 68 (emphasis added).

If the Board has any doubt about the chaos that will ensue, it should study the experience of Florida counties in 2002. Like New York today, Florida was in a rush to implement new technology in that year (there to erase perceptions arising from the presidential election of 2000). Unsurprisingly, each of the steps in the process, from promulgating regulations to certifying machines to procurement, took longer than anticipated. As a result, testing and set up of the machines, and training programs, were compressed into the weeks leading up to the primary. *See* Ex. V at 5-7.

A debacle ensued on primary day, depriving thousands of Floridians in Miami-Dade and Broward of the right to vote. Poor quality hardware and software had been purchased because deliberations were rushed, leading to high machine failure rates on Election Day. Because of the time pressure, machines were not properly tested or set up, and also failed for that reason. Untrained poll workers – harassed by angry voters and growing lines – could not fix the problems or, in some cases, operate even properly

---

[18] *See* "N.Y. way behind in voting reforms," *Democrat & Chronicle* (Rochester, NY: Jan. 16, 2006).
[19] *See* "Counties scramble to modernize voting machines," *The Journal News* (White Plains, NY: Jan. 8, 2006).

functioning machines. Thousands of voters gave up and left, many others questioned whether their vote had registered on the machines, and voters and poll workers alike were left in tears.[20] The day was a fiasco that resulted in headlines around the country to the effect that Florida still had not fixed its election problems. *See* Ex. V at 44-47.

The steps New York must take to prevent such chaos are clear. The Board should seek a waiver of the January 2006 deadline imposed by HAVA so that New York can proceed promptly but deliberately.[21] A term of the waiver should be that New York continues to use its approximately 20,000 existing lever machines in the fall 2006 elections. This is a tried-and-true system that can be effective in the short term while better options are evaluated. With our obligation to voters with disabilities in mind, the Board (and all of us) should do everything in our power to ensure accessibility in the fall 2006 elections while we search for optimal long-term solutions.

If a waiver is not possible, then it would be preferable to give the federal government its HAVA money back rather than deprive thousands of New Yorkers of their votes in a critical election. "Time and money should not jeopardize the integrity of our votes." *See* "N.Y. way behind in voting reforms," *Democrat & Chronicle* (Rochester, NY: Jan. 16, 2006).

IV. Conclusion

The Board must safeguard New York from the risk of electoral fraud perpetrated by unscrupulous insiders and from the risk of chaos in the 2006 mid-term primary and general elections. Both of those purposes may be achieved if the Board will take the time to consider the critique of the proposed regulations and the rushed implementation process set forth above, and will act on those suggestions. By taking care to implement voting system standards that meet the state's and HAVA's goals, New York would turn its present challenges under HAVA into a victory for voters' rights. New York will have created a thoughtful voting system that will protect the rights of the state's voters and be looked to as a model by other states.

As ACCURATE notes, "Past elections have eroded public confidence in the trustworthiness, fairness and accuracy of voting systems and ultimately elections. It is imperative to restore public confidence." Ex. E at 36. Given the lack of effective national standards, voters in New York are looking to the State to ensure that each vote is counted as cast and to preserve public confidence that the winner really won. I urge you to do just that.

Thank you for considering these comments.

---

[20] *See* "Florida Sends SOS on Elections," CBS News (Sept. 19, 2002), available at http://www.cbsnews.com/stories/2002/10/17/politics/main525918.shtml.

[21] It is likely that the Board has or will discuss a memorandum of understanding with the U.S. Department of Justice, given DOJ threat of litigation for New York's failure to comply with HAVA. Any MOU that does not account for the issues set forth herein – for example, one which allowed the defective regulations to take effect or the process to be rushed – would be subject to legal challenge for all of the reasons set forth in this letter.

Sincerely,

Larry Rockefeller

Larry Rockefeller

cc: Department of Justice, Civil Rights Division
New York State Attorney General Eliot Spitzer