To: Douglas Kellner

From : Douglas Jones

Date: March 15, 2006

Re: Kellner March 7, 2006 Revised Draft of Voting System Standards

I have reviewed your March 7, 2006 draft revisions to the voting system standards proposed by the New York Board of Elections on February 14, 2006. I refer to your March 7, 2006 draft revisions herein as the "revised standards." You are moving in the right direction. To secure the State's voting systems, there must be rigorous certification criteria and determinations, aggressive security testing, transparency, and accountability from a verified paper ballot trail and otherwise. I offer these comments to help further improve your draft, and I urge your colleagues on the Board to adopt your draft, as improved.

The following are deficiencies that remain in the voting system standards as you have revised them. To facilitate your consideration of these comments, I refer to relevant paragraphs from my affidavits of January 23, 2006 and February 24, 2006.

Section 6209.1 Definitions:

- 2. Audio Voting Feature – the definition in the revised standards is the same exact definition as the original proposed standards. This definition is inaccurate and can lead to voting systems that poorly serve the needs of those with motor impairments. *See* Doug Jones January 2006 Affidavit at ¶ 31.

- 23a. Resident memory – the revised definition is almost identical to the original draft. This definition does not take into account my concern that the resident memory in real voting systems is plainly used for additional purposes and that ballot images are also stored on non-resident memory on many voting systems. Doug Jones January 2006 Affidavit at ¶ 28, *see also* Doug Jones February 2006 Affidavit at ¶ 19.

- 24. Software – This definition, while changed somewhat, remains problematic. The definition conflates material provided by the vendor and subject to testing at the time a voting machines is certified with the configuration files prepared by the county in order to prepare a voting system for a particular election. *See also* Doug Jones January 2006 Affidavit at ¶ 25. This conflation creates the risk that the government's configuration information will come under the umbrella of nondisclosure that has been extended to cover the vendor's software. In general, information about ballot configuration is published in advance of an election, and the electronic representations of this information ought to be public. The only exception to this is security information, for example, passwords, cryptographic keys, and keys used to create electronic signatures. These should be specifically exempted from public disclosure instead of being protected by a sweeping definition of software.

Definitions still missing:

- These revised standards still do not have a definition for "election configuration" and "election configuration file." The revised standards do not address the fact that these files are not properly considered software, *see* Doug Jones January 2006 Affidavit at ¶ 33, or the problems involved with incorporating these terms as part of the "software" definition. Again, the conflation of material provided by vendors and the government's configuration information improperly causes configuration information to come under the umbrella of nondisclosure.

- These revised standards do not provide a definition for "voting booth" as I suggested in my January 2006 Affidavit. *See* Doug Jones January 2006 Affidavit at ¶ 37. I suspect that the fundamental problem here is that New York has been working with integrated voting-machine – booth combinations for a century. The changes made to the proposed wording of 6209.2 D (2) help, but without a definition of voting booth, you have been forced to use awkward wording there.

Section 6209.2 Polling Place Voting System Requirements

- A(1) Requirement for full ballot display on single surface – revised standards do not address my comments that large full-face voting machines can pose problems for individuals with motor disabilities. The existence of this problem has been very well documented in the context of mechanical lever voting machines, and the reduction of such machinery to electronic form has not been shown to reduce this problem. *See* Doug Jones January 2006 Affidavit at ¶ 38.

- A(5) Diagnostic self tests – revised standards do not address the need to cast real test ballots and not provide only for self-tests of the machines, as self-tests fail to test actual input devices, i.e. switches, touch screens and ballot scanners. The language of this section in the revised standards, is essentially the same as the language of the section in the original proposed standards. Self-tests are valuable, but, as pointed out in footnote 6 of the revised standards, "without the entry of test votes in the exact same manner that they will be entered during the actual election, there can be no confidence that the system and vote entry methods will function properly." *See also* Doug Jones January 2006 Affidavit at ¶ 39. Additionally, this language, when examined in connection with the requirement of casting 800 ballots for testing contained in Section 6209.11 C, suggests that the revised standards only require self-tests, which as explained above, is problematic.

- B(2) Accessibility – the accessibility features required here are important, but merely requiring these features is insufficient. Tactile discernible controls plus an audio voting feature can meet the needs of the blind, but only if properly integrated. Tactile discernible controls alone can meet the needs of those with some motor disorders, but only if properly integrated with the normal ballot display. A pneumatic switch can meet the needs of those with other (generally more severe) motor disabilities, but again, only if properly integrated with the ballot display. You need standards that address the effective

use of these features in order to ensure maximal accessibility. *See* Doug Jones January 2006 Affidavit at ¶ 40.

- C(2) Noise level of write-in components – the revised standards still appear to assume that the noise level of write-in components is the only consideration that needs to be addressed in order to guarantee the privacy of a voter who wants to cast a write-in vote. This is clearly not the case; in my experience, many DRE voting systems are inordinately slow when used to cast write-in votes. *See* Doug Jones January 2006 Affidavit at ¶ 41.

- D. Standards for voter privacy – this revised standard addresses some of my comments from my January 2006 affidavit, but because the revised standards do not define "voting booth", it uses the awkward phrase "curtains, screens, shields or other privacy devices." What you need is a definiton of the term "voting booth" as the enclosure provided by or with polling-place voting equipment in order to ensure privacy. Then, you need to require that voting systems incorporate or come with a voting booth that is constructed as outlined in item (1), and finally, you need item (2) to require that, in the event that the voting booth has a door or curtain, this can be operated easily.

- There is a missing requirement, probably D(3), having to do with the privacy of write-in voting. As mentioned in C(2), the use of write-in voting can be revealed by such things as the noise it creates, but this is not the only thing that reveals the use of write-in voting.

- F. Voter Verified Paper Audit Trails (VVPAT) – This is a newly added section that is not in any earlier drafts of proposed standards. I agree that VVPAT should be defined and highlight sections of this definition that need the most work.

    - Item 9(c) appears to belong under item 11, since the information allowing linkage between the VVPAT and electronic record, if remembered by the voter, would allow that voter to prove which ballot was theirs. The wording "not to be memorable to the voter" makes it a bit difficult to infer this.

    - Item 10(a) is not an audit requirement, it must go somewhere else, probably under security requirements or additional requirements.

    - The suggestion of a test-mode indication in the ballot records in item 10(b) is troublesome! The problem here is that it is dangerous to let a system know that it is being tested because this allows the system to detect this fact and behave differently under test than it does under actual use.

    - Items 12 and 13, digital signatures and data export. These requirements should apply equally to precinct-count optical scan systems and to central count optical scan systems! Also, I am a bit puzzled by the idea of a digital signature on each electronic record versus a digital signature on each file. Digital signatures work well only when the item being signed has an information content that is significantly larger than the signature. Typical record formats for electronic ballot images are not too different in size from typical digital signatures. I recommend

consulting with someone who is an expert in digital signature technology before setting this requirement in stone.

- Items 14(d). This could be a poison pill requirement because just about every printer on the market today designed for use with standard printer ports incorporates a microprocessor and at least a small RAM. Even a 1 bit memory in the printer stores information, thus violating the "cannot store information in memory" requirement. Similarly, essentially all printers offer an "are you there" service, wherein they reply "yes" is asked. This really is a service, and it's one you want to support the self-diagnostic function. I suggest that what you want to prohibit is the storage of information and provision of services that are not essential to system function.

Section 6209.3 Additional Requirements for Voting Systems

- F. "The system shall provide a means by which the ballot definition code may be positively verified to ensure that it corresponds to the format of the ballot face." – the revised standard does not address my concern that "it is unclear whether this is something that would be tested as part of pre-election testing or whether this is a requirement that ballot style be encoded on the paper ballot, so that the ballot tabulating machine can determine what style is in use." Doug Jones January 2006 Affidavit at ¶ 47.

- Revised standards do not include a requirement that precinct-count optical-scan tabulating machines include a secure ballot box. *See* Doug Jones January 2006 Affidavit at ¶ 50.

- Revised standards also do not include "requirement that the ballot box connected to a precinct-count optical-scan tabulating machine include an emergency ballot compartment for use in the event of failure of the tabulating mechanism." Doug Jones January 2006 Affidavit at ¶ 51.

Section 6209.4 Application Process

- J. Regarding disclosure of contribution made by vendor or its officers or controlling shareholder – I see that you are beginning to deal with conflicts of interests but this is just a start. The revised standards do not address the conflicts of interest that arise through a vendor's link to certain issues, as opposed to links to candidates. Because issues are in constant flux, we need to make sure that the information about ownership interests in the voting system vendors are always public so that, as the issues change, we can find out whether a conflict exists. We therefore need investigation, determination and public disclosure of the individuals and corporations who hold an ownership or controlling interest in a voting system product or service company. *See* Doug Jones February 2006 Affidavit at ¶ 18. Conflict of interest protections go to the heart of preserving the integrity of our elections.

- The revised standards do not address my recommendations that voting system vendors be required to submit information regarding past or pending court cases involving their

systems or its major components, evidence of fraud, faulty systems or failure to correct past problems, and the vendor's track record in general. *See* Doug Jones February 2006 Affidavit at ¶ 13, ¶ 15-17.

Section 6209.6 Examination Criteria

- The revised standards still do not provide performance requirements. This is a major problem. There is no definition for a certified voting system or standards for what a certified system must be able to do. The absence of these criteria and the means for evaluating companies and their products and services against these criteria makes these regulations meaningless. In this regard, the revised standards do not take into account any of my suggestions laid out in paragraphs 7 through 12 of my affidavit submitted in February 2006.

- D.1.(B)(5) Escrow and Review of Source Code, requires, in section (a) that "all software that is relevant" be escrowed. There is no question in my mind that this includes certification of the underlying operating system inasmuch as large parts of the operating system are intimately involved with the functionality of the voting system; this clearly applies to operating systems such as Windows. This is the only statement of the software made available to the board, so I conclude that this is the software that must be reviewed by the independent expert required in section (e). In some cases, this is a good thing, for example, the Windows operating system has been notorious for security flaws. On the other hand, because the borders of "all software that is relevant" are so broad, it may prove to be an impossible task to certify any voting system at all. Clearly, additional careful thought needs to be put into this issue.

- D.1.(B)(5)(d) is not an escrow and review requirement, but rather, a support documentation requirement or a disclosure disclosure requirement. I suggest that it probably belongs somewhere under D.2, because this information is needed by the public and by the county boards prior to purchase of the system, for example, in order to ask other users about their experience using the system. This section may be intended to partially address my suggestion that vendors be required to supply such information. *See* Doug Jones February 2006 Affidavit at ¶ 14. As written, it is a start, but it but should go further by requiring disclosure of pending actions such as lawsuits. In many ways, the disclosure required here is comparable to that required in a stock prospectus, since a county making a voting system purchase is, in a very real sense, investing in the vendor.

- D.2.(B)(5)(d) Factory repair tasks – this section of the revised standards largely addresses my concern regarding repair tasks done at the factory but it still appears to mainly discourage sending machines to the factory for repairs and does not explicitly address my concern about security if a county board is allowed to perform upgrades on-site. *See* Doug Jones January 2006 Affidavit at ¶ 53. The problem is, there is no general security requirements section where such a requirement can be placed. 6209.2.(F)14 comes close to being a security requirements section, but this applies only to the voter-verified printer.

- The revised standards also do not put forth any requirements for physical security of precinct based equipment. *See* Doug Jones January 2006 Affidavit at ¶ 54 ¶ 64. Again,

6209.2.(F)14 is the closest approximation to a statement of requirements, but it does not provide a basis against which a security expert could operate in carrying out the requirements of 6209.6.D.2.(C)(3). As a result, the experts will be forced to invent their own criteria.

- The security requirements in clause Section 6209.6 D.2.(B)(1)(n) should make it clear that it is not setting security requirements, but rather, it is asking the vendor to more fully describe the security requirements they meet and to specifically document how they satisfy each requirement. This documentation from the vendor probably belongs in an appendix to the certification application**.** *See* Jones Affidavit February 2006, and attached mark-up to draft revised standards.

- The subsection structure of Section 6209.6 remains very hard to follow!

Sections 6209.10 through 6209.14

- These sections govern the routine use of voting systems by the county and do not govern the process of voting system certification or acquisition. It would be appropriate to carefully comb these sections for requirements that bear on certification. Among them, the vendor should be required to document appropriate acceptance tests for each voting system component and, of course, the system must be testable. The certification process should assess this documentation, of course.

- I suggest that a separate document, focusing entirely on the administration of voting systems after acquisition and approval by the state board would be very desirable. If this is done, the bulk of these sections could be moved to that document. *See* Doug Jones February 2006 Affidavit at ¶ 20.

- In my comments here, I have not focused on operational requirements, since acquisition and certification requirements are paramount at the current time. However, I should note that these standards, as written, address system operation only in these last sections, without addressing a number of issues such as how the public right to observe is guaranteed, how the chain of custody for paper and electronic records is guarded, and how machines are to be secured prior to and after voting.

- The operational requirements must restrict election officials to use the voting system in accordance with the procedures established by statute, New York Board of Elections regulations, and the certification documentation approved by the state board. Election officials should not be allowed to get creative and invent new ways to use voting machines. The license to be creative, in this case, allows violation of one-man-one-vote. If an official does have an innovative idea, it must be brought forward to the state board so that the state can decide on it.

Section 6209.10 Acceptance Testing

- The revised standards do not have a provision in this section for statistical quality control methods, which are an important testing tool when large numbers of identical units are

delivered. When a county receives 1000 identical voting machines, all of them should be tested, but some should be selected at random for far more intensive testing. *See* Doug Jones January 2006 Affidavit at ¶ 55.

Section 6209.11 Routine Maintenance and Testing of Voting Systems

- C. Requiring testing of 800 ballots – The requirement that 800 ballots be tested is crazy. As I explained in my January 2006 Affidavit, a real test involving the casting of 200 ballots is expensive to contemplate. *See* Doug Jones January 2006 Affidavit at ¶ 56. The Miami Herald did a study of how long it took voters to use the touch-screen machines in Miami during early voting in October 2004. They found that the typical voter could vote the general election ballot in about 6 minutes. Entering 800 ballots by hand at this rate would take 80 hours, and you need at least one auditor looking over the shoulder of the person entering the test ballots in order to ensure correct ballot entry. As a result, these numbers are only realistic in the context of an automated self-test. Unfortunately, automated self tests cannot detect the kinds of failures that plague machinery that is stored in warehouses for months between uses. You need real testing of touch-screens, push buttons, sip-and-puff devices and paper transport mechanisms, not simulated self-tests. Again, as with questions about the appropriate use of digital signatures, questions about the number of ballots you need to cast to test a system are highly technical. These numbers should not be set by the seat of the pants, but rather, they should be set in consultation with statisticians who understand quality control. Self tests are good, but I am concerned that as written, these standards will not be read as requiring the manual entry of any real test ballots. See ¶ 39 of my January 2006 Affidavit and above, in my comments to Section 6209.2 A(5).

Section 6209.12 Operational and Testing Procedures for Voting Systems

- The consolidation of requirements for testing is good. That said, Section 6209.12 requires additional work. The required testing focuses almost entirely on the tabulating machines themselves, either DRE machines or mark-sense ballot scanners. In fact, a good pre-election test ought to also include the consolidation of totals from the various machines using the election management system, so that the total effect of the pre-election testing is a dress rehearsal for the entire election, including not only voting, but reduction of data to the form in which it will be released to the press and reduction of data to the final form reported in the canvass

Section 6209.13 Submission of Procedures for Unofficial Tally of Results of Election

- This section in the revised standards is almost exactly the same as the original proposed standards. This section fails to take into account my concerns regarding the importance of establishing standards for the security of communicating unofficial results from county boards to the state board and for requiring a paper printout prior to electronic transmission of these results. *See* Doug Jones January 2006 Affidavit at ¶ 61.

Section 6209.14 Demonstration Models

- This section of the revised standards is also essentially the same as the original proposed section. The revised draft version does not address my concern that five years is too short a time period for the requirement that counties provide a model or diagram of the county's voting system to the public, given how frequently Americans move. *See* Doug Jones January 2006 Affidavit at ¶ 62.

Other general areas that the revised standards fail to address include:

- The revised standards do not address requirements for precinct-count optical-scan ballot tabulations to be equipped with secure ballot boxes that are locked and contain emergency ballot compartments with separate locks. *See* Doug Jones January 2006 Affidavit at ¶ 63.

- Members of the state board should be required to be present at and to participate in certification tests. *See* Doug Jones February 2006 Affidavit at ¶ 20.

- The information received and produced by any person designated to act in any way for the state board should be subject to public scrutiny. Sections 6209.4 E, 6209.4 G, 6209.5 A, 6209.6 A, and many others allow the state board to operate through a designee or other authorized examiner; this has the potential to transfer activity out of the public sphere that would be public if it were performed directly by the state board. In the worst case, operating through designees has the potential to reduce the public function of the state board to rubber-stamp approval of reports submitted to it by its designees. I recommend that it be explicitly stated that all materials submitted to a designee or other authorized examiner should have the same status, with regard to public records laws, as if they had been directly submitted to the state board. I also recommend that there be a requirement of timely release of all reports from designees, along with all public information on which they depend, before board meetings at which action is taken on these materials. Public access to final reports is required, but so is access to other records, such as those provided by the vendor to a contractor of the state board.

- The revised standard fails to address shortcomings of FEC/EAC voting system standards. *See* Doug Jones February 2006 Affidavit at ¶ 20. In my tests of the central count and precinct count ballot tabulators made by Diebold and ES&S, I found that both will count marks made outside but in the near vicinity of the voting target. Neither Diebold nor ES&S, in their written materials, documented the fact that the sensitive areas of their tabulators differed from the voting targets, and none of the testing performed under the FEC/EAC voting system standards program required testing of the presence or absence of this feature. The 1990 and 2002 FEC standards, and the 2005 EAC standard only require testing of how optical mark-sense tabulators count ballots where each voting target is either unmarked or marked with the vendor's prescribed mark. No testing is required of markings that differ from the prescribed mark. The New York Times – Washington Post and the Miami Herald – Knight Ridder studies of the ballots from Election 2000 in Florida showed that a small but significant number of voters marked their ballots with marks that differed significantly from the prescribed mark, for example by circling the voting target. I believe that it is essential for the states to deal with this issue; to do so requires that the state use terminology that allows it to be discussed. Your revisions to the

definitions allow these issues to be discussed, but you have yet to take sufficient control over this issue. 6209.3.L correctly defines the acceptable behavior, 6209.6.D.2.(B)(2) requires the vendor to document the behavior, and 6209.12.B requires that this behavior be routinely tested, but you do not limit the behavior. As a result, if two vendors provide identical paper ballots with identical voting targets printed on them, they are permitted to set completely different criteria for what marks in and around these voting targets will be counted, so long as they document this behavior. This flies in the face of HAVA's requirement that the state set clear standards for what is and is not counted as a vote, leaving the issue entirely in the vendor's hands!

Voting System Standards should set forth requirements for oversight/monitoring of work by contractors. The standard focuses on assessing the vendor, with appropriate certification and acceptance testing to monitor the voting system vendor, but there is little discussion of how the state proposes to monitor the various contractors who are hired to help in the certification process. When the state board or the county board takes direct responsibility for the conduct of elections, there is no question of who is responsible. When aspects of the certification process are contracted out to consultants, the state must require monitoring of the quality of their work. The entire testing régime set forth in the proposed voting system acquisition process leaves testing in the hands of the vendor (for pre-qualification tests) and in the hands of designees of the board such as ITAs. How do you propose to assess the quality of their work? Do you propose any mechanism to track defects discovered in their work?

- The voting system standards should address the measurement of the number of voters that the voting machine can handle per hour. These numbers are needed in order to determine how many voting machines must be in place in each precinct to ensure that all eligible voters who want to vote have a chance to do so. For each machine certified for use in the state, someone needs to sit there with a stopwatch and time how long it takes a typical voter to work their way through a typical general election ballot. They should not leave this to the newspapers, as happened in Miami in October 2004, when the Miami Herald did the study at an early voting location and concluded, from their study, that Miami didn't have enough voting machines in place for the expected turnout in the 2004 general election. Worse yet, they shouldn't wait until election day to discover that they didn't have enough machines, as clearly was the case in some Ohio cities in 2004**.**

Douglas W. Jones