To: New York State Board of Elections and Concerned NY Citizens
From: Rebecca Mercuri, Ph.D.
Date: February 22, 2006
Subject: Comments on Draft of Subtitle V, Part 6209, VSS NY State

I was asked to provide input on the Subtitle V, Part 6209, Voting Systems Standards document currently being compiled by the New York State Board of Elections.[1] I have considerable insight on this material that should be helpful, as I had actively been involved in the formal comment rounds of the FEC 2002 Voting System Guidelines and the EAC HAVA Guidelines, and also participated as a member of the IEEE P1583 working group on Voting System Standards. As well, I have spoken at hearings and contributed wording and conceptual material that has been incorporated into numerous Federal and State legislation, as well as Secretary of State and Boards of Election advisories, pertaining to election equipment, especially during the last half-decade.

In this memorandum, I have described numerous flaws in the current draft of the NY State VSS, where salient changes are necessary. Most of these flaws pertain to incorrect wording or misunderstood technical concepts that appear in the NY State draft VSS. I have listed my most serious advisories here in a Highlights section, pointing out areas where guidance is lacking or has been inappropriately applied, and have also included a Details section that notes further important corrections line by line.

Highlights

This set of NY State regulations appears to rely heavily on the Federal voting system guidelines and certification process, which unfortunately do not provide sufficient assurances to guarantee voting system reliability, security, auditability, and so on. These flaws are legacy to the 1990 FEC VSS, the 2002 FEC VSS, the Draft IEEE P1583 VSS, and the EAC HAVA VSG. I have attached here, for your use, earlier public comments that I wrote that illustrate the extent of the problems with the Federal program, and the numerous gaps that (are not yet but) must be addressed in your regulations. These additional documents are footnoted as [2][3] and [4]. In particular, the flaws related to insider and outsider risks (such as via the use of wireless or Internet-connected voting systems), the reliability aspects, and the accessibility features that do not accommodate the vast numbers of home or hospital-bound disabled, must be mitigated. I urge your careful consideration and reading of these supplementary materials, and hope you will incorporate these admonitions into your regulations.

In the NY State document, VVPAT should be defined throughout as a "voter verified paper audit trail." The use of the word "verifiable" has been promoted by certain individuals to subvert the intention of the VVPAT ballots as legal documents of record that certify the votes cast. All VVPAT systems must provide the voter with a chance to review the ballot along with an action that confirms that such review took place prior to casting. The voter's performance of the acceptance action indicates that they "verified" their ballot and accepted its contents as valid. Actually, it would be preferable to use the phrase "voter verified paper ballot" (VVPB) rather than "audit trail" or "paper record"

because each of the latter phrases have also been distorted from their intended meaning as the ballot of record in this context. (Note that in section 6209.2 F, VVPAT is correctly described as "verified," so this word should be consistently used throughout the entire VSS.)

The requirement for self-testing of system status and random simulation of ballot casting (in Section 6209.2 A. (5)) should not be assumed to provide adequate feedback to determine whether a voting system is properly operational. For example, if the system is malfunctioning, its status tests may also be malfunctioning and may not be reliable. Also, it is unlikely that a self-test of ballot casting will reflect all aspects of actual vote registration – for example, vendor components that generate and store ballots internally, typically do not exercise the keypresses or screen inputs, so these must still be manually performed. Optically scanned systems are often only tested with a set of pristine ballots that do not demonstrate the range of variability that typically occurs within the set of hand-generated ballots that would be found from the different individual voters on election day. Systems that are set into a special "test" mode may not be exercising the same code or may be able to detect test sets, thus the actual election set up may be accidentally or intentionally circumvented. Finally, it must be noted that the lack of failure from a self-test is not proof that the system is properly functional, or that ballot configurations have been appropriately handled (for example, if a "vote for 2 out of 5" has been erroneously programmed for "1 of 5" the random ballot set may not exercise the "2 of 5" condition and the misprogramming will not be noted, or may only be revealed after extensive manual perusal of the test sets). Other flaws with the testing requirements are noted below.

Details

It is recommended that the VSS add (or change to) the wording underlined in these notes. Other information is provided for advisory purposes.

Section 6209.1 Definitions

1. Acceptance Test should be applied to voting system software, <u>firmware</u>, hardware, and <u>affiliated data files</u>. In general use, acceptance testing also applies to configuration management – in other words, examination of all components (hardware, software, etc.) to ensure that proper version control has been applied (so that the units reflect the currently certified components) and that serial and component numbers match the distribution lists, etc.

2. ....the ability to cast their vote <u>with assistance from a sound or aural component</u>.

8. Styles include bubble switch, ballot overlay, <u>and capacitance or light-sensor touch-screen machines</u>.

11. Encrypted Copy – could apply to data in addition to programming code. With many types of encryption, it is the decryption (not the encryption) key that is necessary to unscramble the information.

19. Operational Manual – and (c) should also include instructions for ballot programming in compliance with State regulations.

24. is incorrect. Firmware does not reside on a central processing unit. Should read: Resident Vote Tabulation Programming means the manufacturer's firmware programming that resides in the read-only memory components affiliated with the central processing unit. This firmware controls the registering, accumulation and storage of votes and ballot images.

26. is incorrect. Interpreted code is not allowed by the EAC Voting System Standards. Machine language is not what is being executed by the computer. The second sentence should read: Source Code is not executed by the computer directly, but is converted into object code by compilers and assemblers.

33. VVPAT see Highlights comment (above). Use verified not verifiable.

Section 6209.2 Polling Place Voting System Requirements

A. (2) ... voter verified permanent paper record

A. (4) Add this sentence at the end: The batteries should not be required to be continually charged (or "plugged in") while the voting devices are in storage.

A. (5) See Highlights comment (above) about the inadequacy of this requirement.

A. (6) Add sentence at end: Procedures must be specified thoroughly to deal with each type of condition where the contents of some or all of the redundant memory systems have been invalidated, have experienced a failure, or do not agree.

A. (7) Add sentences at end: The voter must be provided with an opportunity to change overvoted or undervoted selections prior to casting the ballot. For optically scanned systems, this should require notification of the voter of the procedure whereby they can void their ballot and obtain a new blank one.

B. See Highlights comment (above) about accessibility design issues.

C. Add (3) If a voting system uses an audible (i.e. sound) alert to poll workers, indicating that the voter has cast their ballot, this should also be accompanied by a visual (i.e. light) indicator in case a momentary noise level obscures the audible alert.

D. (1) Should be more specific about the distance away from the equipment where no one can see the vote. And should add: (except for the voter).

F. 1. (a) change to: The paper record shall be considered the voter's cast ballot of record, reflecting the voter's complete selection of ballot choices, to be used ...

F. 4. add as (b) If the voter rejects the printed ballot, they shall be entitled to recast their vote up to the maximum number of recasts allowed.

F. 4. change (b) to (c) and reword: Prior to reaching the maximum number of recasts allowed, ...

F. 6. ...shall be documented and posted at the polling station.

F. 8. Since it is unclear what is meant by "returning a voting system to correct operation" wording must be added to this section as follows: For this procedure, controls must be provided to ensure that no actions can be performed that could compromise the integrity of the electronic and paper ballots already stored, or that could allow additional votes to be cast by anyone other than the subsequently authorized voters.

F. 9. (b) ....whose paper records contain any of the alternative languages or font sizes chosen....

F. 9. (c) must be changed to: There shall appear no auditing marks, numbers, or codes on the ballot that can be used in any way whatsoever, by any person (including the voter), to later identify their cast ballot. Note that even very long alphanumeric strings (such as are currently being generated by some of the vendors) printed on the ballot could be copied down by the voter during the verification process, so this must not be allowed.

F. 10. It is unclear why this item, along with its sub-sections (a) and (b) are contained within the VVPAT section – the ballot records should be structured and contain information to support highly precise audits of their accuracy regardless of whether VVPAT is used or not, so this should be moved to a general section of the VSS. Furthermore, sub-section (a) pertaining to cryptographic software should be reworded: All cryptographic software in the voting system shall be identified by module, component, and algorithm, and shall have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable. The vendor must supply instructions as to how the cryptographic modules will be updated if/when the algorithm has been determined to be breachable in general use.

F. 11. *The draft wording here must be removed*. Note that the application of a unique identifier to the printed ballot can violate voter privacy (see notes on F. 9. (c) above). Since the VVPAT is the actual ballot of record, it is not necessary to link it to the electronic record. In cases of discrepancy, it should be the VVPAT totals that prevail. Furthermore, the intention of the VVPAT is to provide an *independent* way of verifying the vote totals. If the VVPAT records are linked to the electronic records in any way, this independence is lost.

F. 12. ... but this digital signature shall not be able to be used to violate voter privacy.

F. 13. (a) replace non-priority format with non-proprietary format. Eliminate "and should be in a format that is commonly used by electronic voting system manufacturers" (since currently no such format exists between vendors, and none may be agreed upon in the foreseeable future).

Add to Section 6209.2 the following: The system must ensure, and testing must validate, that cast ballot maximums that, if exceeded, could result in overflow conditions that may adversely affect stored ballot data and vote totals, must be physically prevented from occurring by the voting system. Procedural controls to prevent overflow shall be deemed insufficient.

Add to Section 6209.2 the following: The system must ensure, and testing must validate, that no component of the system can be reprogrammed, nor its ballot configuration altered, at any time, from the beginning of ballot casting through the end of vote totaling. The system shall further ensure that no ballot or keypress or device may be entered that shall be allowed to trigger reprogramming or reconfiguration during election operations.

Add to Section 6209.2 the following: The same level of examination and testing for COTS components is as required for all other parts of the voting system. Furthermore, all COTS components must be identified as such, and the vendor shall agree to notify the State Board and all purchasers of all defects or recalls of COTS products that could adversely affect voting system operations in any way.

Section 6209.3 Paper-based Voting Systems

A. Add: (4) The system must be able to correctly handle all allowable variations of vote choice within contests (i.e. vote for m of n).

I. (1) and (2) need to be changed. As noted (in Highlights and in the above Section), the allowance of COTS components in voting systems without thorough examination is a serious flaw in the FEC 2002 and EAC HAVA voting system guidelines. The same level of examination and testing for COTS components is as required for all other parts of the voting system. Furthermore, all COTS components must be identified as such, and the vendor shall agree to notify the State Board and all purchasers of all defects or recalls of COTS products that could adversely affect voting system operations in any way.

J. (3) add at end: identify different ballot styles in an unambiguous way.

Add to Section 6209.3 the following: The system must ensure, and testing must validate, that cast ballot maximums that, if exceeded, could result in overflow conditions that may adversely affect stored ballot data and vote totals, must be physically prevented from occurring by the voting system. Procedural controls to prevent overflow shall be deemed insufficient.

Add to Section 6209.3 the following: The system must ensure, and testing must validate, that no component of the system can be reprogrammed, nor its ballot configuration altered, at any time, from the beginning of ballot casting through the end of vote totaling. The system shall further ensure that no ballot or keypress or device may be entered that shall be allowed to trigger reprogramming or reconfiguration during election operations.

Add to Section 6209.3 the following: All cryptographic software in the voting system shall be identified by module, component, and algorithm, and shall have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable. The vendor must supply instructions as to how the cryptographic modules will be updated if/when the algorithm has been determined to be breachable in general use.

Section 6209.5 Submission of Voting Systems Equipment

A. Add sentence at end: Vendor shall supply a comprehensive Risks Analysis and mitigation for the voting system and all components, addressing breaches by authorized and unauthorized personnel and other vulnerabilities.

Section 6209.6 Examination Criteria

A. Add at end: The testing laboratory shall be required to disclose any conflicts of interest they may have with regard to prior or existing voting system vendor contracts.

B. Physical Configuration Audit (4) Strike entire sentence: At the conclusion of the examination the State Board or its designee shall return to the vendor all such documentation and shall not retain any copies thereof. Replace with: The State Board shall escrow all information designated as proprietary by the vendor, and vendor shall agree to disclosure if requested for a court or government proceeding.

C. Note that (currently) the EAC does not perform the accreditation of the ITAs, this is (now) done by NASED. Due to potential conflicts of interest, and the lax accreditation for the ITAs in the Federal program, it would be preferable that NY engage non-ITA laboratories for additional State certification testing. For example, labs accredited under other recognized industry programs might be considered.

C. 1. As noted above in the Highlights advisory, the "tests performed at the federal level" are inadequate in providing sufficient assurances so the State Board must ensure that supplemental testing closes gaps that have been unaddressed.

C. 1. A. As well, the functional configuration audit is, in itself also inadequate in revealing all flaws, as blackbox testing can not fully "exercise all system functions" and "detect program logic and data processing errors." Audit procedure must therefore include NY State creating its own tests, in addition to those supplied by the vendor. The physical configuration audit must also include independent builds of the various software and firmware components from the source code supplied by the vendor.

C. 1. A. (2) add (d) a comprehensive set of data flow diagrams for all modules and components.

C. (2) ... error conditions which may result from hardware malfunctions, and also indicate the set of conditions that are not detectable during hardware malfunctions.

C. 2. (B) (1) Software Specification (q) ... exception handling ... (not "exceptional")

C. 2. (B) (1) Software Specification: items should be added to also address the cryptographic configurations and recalls, the COTS configurations and recalls, and the Risks Assessment and mitigation. (See my discussion of these items within other Section notes in this document.) Note that the Risks Assessment noted as optional in the vendor Appendices (s of this section) should instead be required.

C. 2. (B) (3) Maintenance Information (b) add: All custom parts that are not generally available shall be identified along with information regarding substitution and obtainability.

Section 6209.8 Rescission of Certification

A. add 1. All voting system vendors are required to provide the State and all NY purchasers with timely notice of any defect or condition that could adversely affect its certification or proper operation, whether or not this defect or condition was observed in NY State.

Add F. Any voting system or component that has been decertified three times in a given calendar year shall be precluded from recertification or use until a full calendar year has elapsed from the time of its last decertification.

Section 6209.9 Contracts

A. (1) (a) ... and acceptance testing in accordance with State Board requirements (as per section 6209.10) of such equipment;

A. (1) (c) ... operations and procedural manuals... Note that there may be procedures that need to be specified beyond those given for the poll workers.

A. (1) add at end of (e) ballot face layout and ballot programming, vote tally reconciliation and auditing, and county-wide election tally reporting.

A. (2) add at the end of (e): , without additional cost and whether or not the problems or defect were detected by purchaser.

A. (2) add (g) The vendor and purchaser shall agree in writing as to the manner in which the costs of a re-election, should one become necessary due to defect in equipment or

performance, will be shared. This could include the posting of a bond or guarantee of insurance coverage.

A. (2) add (h) The vendor shall specify the contingency provisions that will be observed, should the equipment be decertified during an election cycle.

A. (3) (a) ...meet environmental and engineering conditions for the proper operation....

A. (4) (be) ... acceptance testing in compliance with State Board requirements (as per Section 6209.10).

Section 6209.10 Acceptance Testing

E. ... the vendor must make corrections, at its own expense, to ...

F. add at end: Municipalities that had purchased such rescinded equipment shall be entitled to terminate procurement and maintenance contracts, receive a full fund of any purchase payments already made (upon return of equipment and materials already delivered), and seek compensation from the vendor for any additional costs incurred (including any excess charges related to the purchase of replacement voting systems).

Section 6209.11 Routine Maintenance Test of DRE Voting Systems

C. ... the manual casting of a minimum of 200 ballots, exercising the broadest possible range of office configurations and ballot choices, on each piece of equipment, running in the mode that would be used on election day, during ...
G. add (1) Equipment that does not demonstrate 100% accuracy in vote recording and tallying, has been discovered to be configured improperly, or demonstrates any other defect that affects proper operation, shall be withdrawn from use until remediation and retesting has occurred.

Section 6209.12 Operational and Testing Procedures for Centrally-Counted Paper-based Voting Systems

B. ... processing a manually prepared test deck for each ballot style that exercises the broadest possible range of vote choices using a wide variety of marking devices (pencil, pen, different inks, etc.).

B. add (1) Equipment that does not demonstrate 100% accuracy in tallying, has been discovered to be configured improperly, or demonstrates any other defect that affects proper operation, shall be withdrawn from use until remediation and retesting has occurred.

E. This item, as worded, can not be considered a proper demonstration of operations, and further could introduce risks of vote total contamination, so this type of testing should not be allowed. If deemed necessary, the vote totaling process should just be stopped, a

results printout provided (or voided), a post-election test run (as described in F), the equipment cleared, and a subsequent batch of ballots scanned. *Point E here should be eliminated.*

G. (2) add at end: Following vendor repair, any tabulation that had been stopped must be voided and started from the beginning, with all interim totals discarded, and all ballots from the interim set rescanned.

Section 6209.14 Demonstration Models

Note: The demonstration model is intended for use by a voter unfamiliar with the actual voting equipment to be able to be shown or to practice how to vote, in a generic way. Therefore, the demonstration model must provide no misleading information that could confuse a voter into incorrectly casting a vote when using the actual device and an official ballot. Nor can the model omit any salient step or sequence that the voter would be need to understand in order to perform proper vote selection and casting. *This wording needs to be reflected in the section.*

References

[1] http://www.elections.state.ny.us/hava/2ndDraftVotingMachineRegs.pdf

[2] Mercuri, Rebecca, "The FEC Proposed Voting Systems Standard Update," September 10, 2001, http://www.notablesoftware.com/Papers/FECRM.html. Attached as file: FECVSS2002Mercuri.pdf

[3] Mercuri, Rebecca, "Lack of Security Assurances and Auditability Requirements in the IEEE P1583 Draft 5.3.2 Voting System Standards," December 20, 2004. Attached as file: MercuriEACmemo.pdf

[4] Mercuri, Rebecca, "EAC Voting System Guidelines Comments," September 30, 2005. Attached as file: VVSGComment.pdf