New York State Technology Enterprise Corporation

NYSTEC Review of CIBER Master Test Plan and CIBER Security Master Test Plan

New York State Board of Elections

Submitted to:

New York State Board of Elections
40 Steuben Place, Albany NY 12207

September 27, 2006
Version 1

Confidential

Table of Contents

1. EXECUTIVE SUMMARY

The NYS Board of Elections (NYSBOE) requested that NYSTEC provide an independent security related review of CIBER's Security Master Test Plan. This review assumes that security testing must include all security related requirements in the 2006 NYS Election Law, EAC 2005 VVSG Vol 1 & 2, and NYS 6209 regulation. The review identified the security related requirements in these four source documents and attempted to match them to the requirements in the test plan. In conducting this review, NYSTEC found it necessary to also comment on CIBER's Master Test Plan. This document presents NYSTEC's review findings of the two CIBER documents.

In summary, the CIBER Security Test Plan presents at a high level CIBER's approach to security testing. In reviewing the Security Master Test Plan, NYSTEC found security requirements that are in the 2006 NYS Election Law, EAC 2005 VVSG Vol 1 & 2, and NYS 6209 regulations that were not covered in the Security Test Plan (details documented below). Other significant findings were that many of the security related requirements were in the Master Test Plan but not in the Security Master Test Plan and that the security test plan did not specify any test methods or procedures for the majority of requirements.

A Security Master Plan should document testing methodologies, procedures and processes that will help to ensure that all testing is being done in a structured and repeatable way. This is even more important given the numbers of voting machines that will be tested in parallel and the numbers of testers involved.

NYSTEC strongly recommends that all the findings in this review be incorporated into the final Security Master Test Plan.

2. REVIEW OF CIBER MASTER TEST PLAN

In order to put the issue in perspective, two primary questions were discussed at length. These questions and discussions concerning them constitute the two subsections that follow.

2.1 General Findings in CIBER Master Test Plan

- The Master Test Plan strives to include all requirements (functional and security) from the 2005 VVSG and the NYS 6209 regulations. In many cases, the security requirements contained in the Master Test Plan are not included in the CIBER Security Master Plan. ***Suggestion: Update the Security Master Test plan to include all security-related requirements from the Master Test Plan.***
- Appendix A lists the requirements and standards to which NYSBOE holds voting systems. The list also should include the 2006 NYS Election Law requirements. ***Suggestion: Include all relevant requirements from the NYS 2006 Election Law in the CIBER Master Test Plan.***
- Generally, there are substantial overlaps between the CIBER Master Test Plan and the CIBER Security Master Test Plan; is this the intention? Should the Security Master Test Plan simply reference the Master Test Plan if, in

fact, the Master Test Plan is intended to document all tests that will be performed on the systems, or is the Security Master Test Plan a subset of the Master Test Plan with security requirements extracted for convenience? ***Suggestion: This issue should be clarified to ensure that security and functionality testers test for the appropriate requirements. The purposes of each plan should be stated, so they are well understood by the BOE and NYSTEC.***

- Under Anomaly processing, the term *cosmetic failure* (page 33) is used. What is considered a cosmetic failure and what is not. ***Suggestion: define this term.***
- In Appendix B. Unclear whether the appendix is meant to be an outline, or the actual test scenarios? Will the detailed testing procedures be part of this Appendix, or will they be provided as a separate document?
- In Appendix C, TDP Initial Matrix. CIBER states that the table needs to be updated to reflect the 2005 FEC/EAC Guidelines. NYSTEC was not able to review the Table's compliance with 2005 FEC/EAC guidelines. ***Suggestion: Update the table.***
- In Appendix D, Required Functions. Unclear what this refers to, does it refer to the "Functional Qualification Matrix"? ***Suggestion: This section needs to be completed.***
- In Appendix A1, Functional Requirements, the following requirements are incorrectly labeled: 6209.3.l.a.1-3 should be 6209.3.a.1-3.

2.2 Specific Findings related to CIBER Master Test Plan

2.2.1 Findings from the NYS 6209 Regulations

Appendices A.1 Functional requirements, A.2 TDP Requirements, and A.3 Source Code Standards contain the requirements from 6209. ***The following requirements do not appear in the CIBER Master Test Plan:***

6209.2.F.10.a ***This requirement should appear in the CIBER Security Master Test Plan***

6209.2.F.14.b,c,d,e,g ***These requirements should appear in the CIBER Security Master Test Plan***

6209.2.G ***This requirement should appear in the CIBER Security Master Test Plan***

6209.2.H ***This requirement should appear in the CIBER Security Master Test Plan***

6209.6.F.4 ***This requirement should appear under the functionality section of the CIBER Master Test Plan.***

Note: During the review for the inclusion of security related requirements from the 6209 regulations, NYSTEC noticed that the functional requirements in the list that follows are not present in the CIBER Master Test Plan.

6209.2.A.5

6209.2.A 6

6209.2.A 9

6209.2.B.1

6209.2.B.3

6209.2.C.1-2

6209.2.D.1-2

6209.2. E

6209.2.F.15 a,b,c,d ii (question what is a state-approved container?)

6209.2.F.18

6209.2.I

In Appendix A.2 TDP Requirements - The requirements ask the vendor to provide documentation. It appears that the test is whether or not the documentation has been provided as per the TDP,

2.2.2 Findings from the Federal VVSG Guidelines

While reviewing the Master Test Plan for security related items we noted that a one for one mapping of the functional testing "that is not security related" needs to be done to validate that all requirements in the VVSG are addressed.

2.2.3 Findings from NYS 2006 Election Law

The following section lists requirements from the 2006 NYS Election Law that should be tested for in either the CIBER Master Test Plan or the CIBER Security Master Test Plan.

7-202. Voting machine or system; requirements of.
1. A voting machine or system to be approved by the state board of elections shall:
a. be constructed so as to allow for voting for all candidates who may be nominated and on all ballot proposals which may be submitted and, except for elections at which the number of parties and independent bodies on the ballot exceeds the number of rows or columns available, so that the amount of space between the names of any two candidates of any party or independent body in any row or column of such machine or system at any election is no greater than the amount of space between the names of any other candidates of such party or independent body at such election;
Suggestion: Include in CIBER Master Test Plan

b. permit a voter to vote for any person for any office, whether or not nominated as a candidate by any party or independent body without the ballot, or any part thereof, being removed from the machine at any time;
Suggestion: Include in CIBER Master Test Plan

c. be constructed so that a voter cannot vote for a candidate or on a ballot proposal for whom or on which he or she is not lawfully entitled to vote;
Suggestion: Include in CIBER Master Test Plan

d. if the voter selects votes for more than one candidate for a single office, except where a voter is lawfully entitled to vote for more than one person for that office, notify the voter that the voter has selected more than one candidate for a single office on the ballot, notify the voter before the ballot is cast and counted of the effect of casting multiple votes for the office, and provide the voter with the opportunity to correct the ballot before the ballot is cast and counted;
Suggestion: Include in CIBER Master Test Plan

e. provide the voter an opportunity to privately and independently verify votes selected and the ability to privately and independently change such votes or correct any error before the ballot is cast and counted;
Suggestion: Include in CIBER Master Test Plan

f. be provided with a "protective counter" which records the number of times the machine or system has been operated since it was built and a "public counter" which records the number of persons who have voted on the machine at each separate election;
Suggestion: Include in CIBER Security Master Test Plan

g. be provided with a lock or locks, or other device or devices, the use of which, immediately after the polls are closed or the operation of the machine or system for such election is completed, will absolutely secure the voting or registering mechanism and prevent the recording of additional votes;
Suggestion: Include in CIBER Security Master Test Plan

h. be provided with sufficient space to display the information required herein, provided, however, in the alternative, such information may be displayed within the official ballot;
Suggestion: Include in CIBER Master Test Plan

i. be provided with a device for printing or photographing all counters or numbers recorded by the machine or system before the polls open and after the polls close which shall be a permanent record with a manual audit capacity available for canvassing the votes recorded by the machine or system; such paper record shall be preserved in accordance with the provisions of section 3-222 of this chapter;
Suggestion: Include in CIBER Security Master Test Plan

j. retain all paper ballots cast or produce and retain a voter verified permanent paper record which shall be presented to the voter from behind a window or other device before the ballot is cast, in a manner intended and designed to protect the privacy of the voter; such ballots or record shall allow a manual audit and shall be preserved in accordance with the provisions of section 3-222 of this chapter;
Suggestion: Include in CIBER Security Master Test Plan

k. provide sufficient illumination to enable the voter to see the ballot;
Suggestion: Include in CIBER Master Test Plan

l. be suitable for the use of election officers in examining the counters such that the protective counters and public counters on all such machines or systems must be located so that they will be visible to the inspectors and watchers at all times while the polls are open;
Suggestion: Include in CIBER Master Test Plan

m. be provided with a screen and hood or curtain or privacy features with equivalent function which shall be so made and adjusted as to conceal the voter and his or her action while voting;
Suggestion: Include in CIBER Master Test Plan

n. contain a device which enables all the election inspectors and poll watchers at such election district to determine when the voting machine or system has been activated for voting and when the voter has completed casting his or her vote;
Suggestion: Include in CIBER Master Test Plan

o. permit the primaries of at least five parties to be held on such machine or system at a single election, and accommodate such number of multiple ballots at a single election as may be required by the state board of elections but in no case less than five;
Suggestion: Include in CIBER Master Test Plan

p. be constructed to allow a voter in a wheelchair to cast his or her vote;
Suggestion: Include in CIBER Master Test Plan

q. permit inspectors of elections to easily and safely place the voting machine or system in a wheelchair accessible position;
Suggestion: Include in CIBER Master Test Plan

r. ensure the integrity and security of the voting machine or system by:
(i) being capable of conducting both pre-election and post-election testing of the logic and accuracy of the machine or system that demonstrates an accurate tally when a known quantity of votes is entered into each machine; and
(ii) providing a means by which a malfunctioning voting machine or system shall secure any votes already cast on such machine or system;
Suggestion: Include in CIBER Security Master Test Plan

s. permit alternative language accessibility pursuant to the requirements of section 203 of the Voting Rights Act of 1965 (42 U.S.C. 1973aa-1a) such that it must have the capacity to display the full ballot in the alternative languages required by the federal Voting Rights Act if such voting machine or system is to

be used where such alternative languages are required or where the local board deems such feature necessary; and

Suggestion: Include in CIBER Master Test Plan

2. The state board of elections shall approve, for use at each polling place at least one voting machine or system at such polling place which, in addition to meeting the requirements in subdivision one of this section, shall:

a. be equipped with a voting device with tactile discernible controls designed to meet the needs of voters with limited reach and limited hand dexterity;

b. be equipped with an audio voting feature that communicates the complete content of the ballot in a voice which permits a voter who is blind or visually impaired to cast a secret ballot using voice-only or tactile discernible controls; and

c. be capable of being equipped with a pneumatic switch voting attachment which can be operated orally by gentle pressure or the creation of a vacuum through the inhalation or exhalation of air by the voter including, but not limited to, a sip-and-puff switch voting attachment.

Suggestion: Include in CIBER Master Test Plan

3. REVIEW OF CIBER SECURITY MASTER TEST PLAN

3.1 General Findings in CIBER Security Master Test Plan

- The first paragraph in the document does not mention that physical security features and controls will be tested. The paragraph does state that electronic and computerized security features will be tested. ***Suggestion: Update wording to include the testing of physical security features.***
- In the Overview and Approach section, the first paragraph seems to infer that the work is primarily a risk assessment. This is not NYSTEC's understanding of the work. NYSTEC views this work to be performed as a sequence of tests designed to test each machine's compliance (pass or fail) with Federal and NY State security requirements. ***Suggestion: Update wording to reflect this and discuss.***
- On page 6, where the compliance-scoring system is discussed, it is unclear to NYSTEC how and when the "N/A" compliance indicator will be used. "N/A" should not mean two different things. ***Suggestion: Clarify***
- On page 8, under the "examine" section, the importance and use of vendor Technical Description Packages (TDPs) should be mentioned, because much of the "examine" work will utilize these documents. ***Suggestion: Update wording to reflect this.***
- The Security Test Planning subsection (under the Overview and Approach section) of this document talks about developing a comprehensive test plan, which should address the following:
  - System Familiarization - the plan does not outline procedures or steps to become familiar with machines in order to complete the testing. ***Suggestion: Include procedures and recommendations to achieve a system familiarization level that is sufficient for conducting security tests.***
  - Creation of a Security Requirements Traceability Matrix - the plan does not provide a specific reference back to either the Master Test Plan or the specific requirements from the federal and state documents. Only references to major sections are provided. ***Suggestion: As needed, provide references (as was done in the CIBER Master Test Plan) to the specific federal or state requirement (not just to applicable section) or reference back to the CIBER Master Test Plan. Many security-related tests are present in the Master Test Plan, but not listed in this plan.***
  - Selection of Test Methods - although stated as a component of the test plan, the test methods to be used are not indicated throughout the plan. The plan states that the selection of the test method is a joint effort between CIBER and NYSTEC. NYSTEC's understanding of NYSTEC's role in the project is that CIBER provides suggested test methods and NYSTEC will review and comment on them. ***Suggestion:***

It would seem that many of the test methods (i.e., those that are not machine specific) should be documented in the plan at this time. Change wording on NYSTEC's role.

- Development of Test Scripts - although stated as a plan component, there is no such section at this point. ***Suggestion: If possible at this phase, include the test-script-development process/outline in the Security Test Plan.***

- The Security Master Test Plan includes three requirements from the 2006 NYS Election Law, but is missing other security-related requirements from the NYS Election Law. ***Suggestion: Review the entire NYS 2006 Election Law — in particular sections 7-200 to 7-209 — and include all security-related requirements in the Security Master Test Plan. Map requirements to the specific Election Law location in all test cases.***

- The Security Master Test Plan does not include many security tests — e.g., those from the NYS Regulations 6209.6.F.3.n1 — that are included in the Master Test Plan. The entire Security Master Test Plan makes only one reference to 6209. ***Suggestion: The Security Master Test Plan should be updated to include all security-related tests from the NYS 6209 regulations, and should provide mappings to the specific regulation requirements.***

- The Security Master Test Plan does not include many VVSG required security tests — e.g., VVSG Vol 1 Sec.2.1.1g — that are included in the Master Test Plan. ***Suggestion: Update plan to include all security related tests that are required by VVSG.*** The Security Master Test Plan does not include many security tests — e.g., those from the NYS Regulations 6209.6.F.3.n1 — that are included in the Master Test Plan. The entire Security Master Test Plan makes only one reference to 6209. ***Suggestion: Vol 1 and Vol 2.***

- Throughout the plan, there are tests that are mapped to "CIBER Security: Secure Coding Practices" or simply "CIBER". This may be beneficial, as CIBER, based on its past experience and expertise, is conducting additional tests that will augment the Federal Guidelines. Will, however, these requirements be viewed as being at the same level of importance as the other State and Federal requirements? Will a vendor fail if it is unable to meet a CIBER requirement? For example, Req # 3.37 is fairly broad and may include cryptographic capabilities that are not utilized in NYS. ***Suggestion: Clarify this issue with BOE and map any CIBER test requirements to appropriate State or Federal documentation. Additionally, these CIBER requirements can also be interpreted as procedures for testing software.***

- The Security Master Test Plan should contain a section on how the source code analysis will be conducted. This would seem to be a component the plan needs in order to ensure that all source-code reviewers follow similar processes. This would seem to be an important plan component, because many reviewers will be used in parallel to perform the source-code review,

and ideally they should follow similar testing processes. This plan should address process steps such as the use of automated scanning software, focus areas, source code review process, order of tasks, etc. Each test under the Software Security Requirements section does contain an area in which to describe the test procedure; however, none of these areas are populated. The Security Master Test Plan should have this level of detail at this point for many of the source-code tests. ***Suggestion: Use EAC 2005 VVSG Vol 2, Section 5, Software Testing, as a basis for this section of the Security Master Test Plan. It is also suggested that, where possible, the test procedure be documented for each test under the Software Security Requirements section.***

- The last paragraph on page 5 of this document discusses the use of color codes to indicate the level of compliance or noncompliance with each security control; however, it is not clear how — during the testing process and/or in the final reports — color and the other indicators (Compliant, Partially Compliant, or Non-Compliant) will be utilized together. Will these colors be used: 1) to indicate a level of compliance or risk that is associated with each requirement that is marked "Partially Compliant" or 2) will the color scale be used to indicate a risk level associated with other findings outside of the test matrix requirements? ***Suggestion: CIBER should describe in the plan how this marking system will be used.***

- At the top of page 10 in the plan, there appears to be a sentence ("The assessment method attributes…") and a bulleted item that are out of place and possibly left in by mistake from the previous version when the section on impact level was deleted. ***Suggestion: Verify the need for this, and make the appropriate correction.***

- It is unclear to NYSTEC what the purposes of the "documented dependencies" section is in each test. ***Suggestion: Please clarify.***

- The section on "Telecommunication and Data Transmission Security Requirements" has several duplicate requirements, as well as requirements that do not map to anything. Additionally, the tests in this section should show that the networking devices do not exist, because saying to disable them is not truly relevant. (Check with BOE on this.) ***Suggestion: Remove the duplicate requirements, map the remaining requirements, and verify with BOE if removing a network or wireless component is required, or if disabling the functionality will satisfy the requirement.***

- The inclusion of several NIST SP800-53 requirements will add to the value of the security testing; however, are these requirements of the voting machine when they do not match up with similar NYS or federal requirements? If these types of requirements are to be evaluated and included in the final reports, they should be marked as "criteria not needed for certification."

- The Security Master Plan should provide a high-level description of testing procedures and plans for machine compliance with Section 7 of the VVSG Vol 1 2005 Guidelines.

3.2 Specific Findings in CIBER Security Master Test Plan

3.2.1 Findings from the NYS 6209 Regulations

- In places, the mapping is to New York State Voting Requirements or NY State Requirements – unclear whether this references 6209. ***Suggestion: Clarify mapping.***
- No mapping of the stated requirements exists to particular sections of the 6209 or to New York State Election law, e.g., requirements # 2.19, 2.20, 3.35, 3.38, 3.38 (there are two 3.38 tests).
- 6209.2.F.10 (a)
  All cryptographic software in the voting system shall have been approved by the U.S. Government's Crypto Module Validation Program (CMVP) as applicable.
  Question: **Is this being done by a code review, or by verifying with an on-line database of crypto modules that have passed certification?** ***This requirement should appear in the CIBER Security Master Test Plan.***
- 6209.2.F.
  (11) In the case of a DRE voting system, the electronic and paper records shall be linked by including a unique identifier within each record that can be used to identify each record uniquely and correspond the two accordingly.
  (12) The voting system shall generate and store a digital signature for each electronic record.
  (13) The electronic records shall be able to be exported for auditing or analysis on standards-based and/or information technology computing platforms.
  (b) The voting system shall export the records accompanied by a digital signature of the collection of records, which shall be calculated on the entire set of electronic records and their associated digital signatures. ***Question: How will these tests be performed. This requirement should appear in the CIBER Security Master Test Plan.***
- **6209.2.G -** Any submitted voting system's software shall not contain any code, procedures or other material which may disable, disarm or otherwise affect in any manner, the proper operation of the voting system, or which may damage the voting system, any hardware, or any computer system or other property of the State Board or county board, including but not limited to 'viruses', 'worms', 'time bombs', and 'drop dead' devices that may cause the voting system to cease functioning properly at a future time. ***Suggestion: This requirement should appear in the CIBER Security Master Test Plan***

- **6209.2.H** –Any submitted voting system shall provide methods through security seals or device locks to physically secure against attempts to interfere with correct system operations. Such physical security shall guard access to machine panels, doors, switches, slots, ports, peripheral devices, firmware, and software. ***Question: How will this be tested for?***

- **6209.6.D.3.c** - The State Board or its designee shall review the vendor's source code and documentation to verify that the software conforms to the documentation, and that the documentation is sufficient to enable the user to install, validate, operate and maintain the voting system. The review shall also include an inspection of all records of the baseline version against the vendor's release control system to establish that the configuration, being qualified, conforms to the engineering and test data. ***Question: How will this be tested for? Suggestion: This requirement should appear in the CIBER Security Master Test Plan.***

- **6209.6.F.3.k** - The vendor shall also describe the capabilities and methods for detecting and handling exceptional conditions, system failure, data input/output errors, error logging and audit record generation and security monitoring and control. ***Question: Included in TDP.??? What tests will be conducted to compromise the correct system operation in order to test these capabilities?***

- **6209.6.F.3.n** - Security requirements and security provisions of the system's software shall be identified for each system function and operating mode. The voting system must be secure against attempts to interfere with correct system operation. The vendor shall identify each potential point of attack. For each potential point of attack, the vendor shall identify the technical safeguards embodied in the voting system to defend against attack, and the procedural safeguards that the vendor has recommended be followed by the election administrators to further defend against that attack. Each defense shall be classified as preventive, if it prevents the attack in the first place; detective, if it allows detection of an attack; or corrective, if it allows correction of the damage done by an attack. Security requirements and provisions shall include the ability of the system to detect, prevent, log, and recover from the broad range of security risks identified. These procedures shall also examine system capabilities and safeguards claimed by the vendor to prevent interference with correct system operations. The State Board, with the assistance of its ITA, shall conduct tests to confirm that the security requirements of these Regulations have been completely addressed. Notwithstanding any other provisions of these Regulations, the State Board shall determine whether all or a portion of such security requirements and security provisions shall be available for public inspection, but shall exclude any information that compromises the security of the voting system. ***Question: How will this be tested for?***

- 6209.6.F.3

(o) Programming Specifications - The vendor shall provide an overview of the software design, structure, and implementation algorithms. Whereas the Functional Specification of the preceding section provides a description of what functions the software performs and the various modes in which it operates, this section should be prepared so as to facilitate understanding of the internal functioning of the individual software modules. Implementation of functions shall be described in terms of software architecture, algorithms, and data structures, and all procedures or procedure interfaces that are vulnerable to degradation in data quality or security penetration shall be identified. ***Question: How will this be tested for? Suggestion: This requirement should appear in the CIBER Security Master Test Plan.***

(p) Test and Verification Specifications

The vendor shall provide a description of the procedures used during software development to verify logical correctness, data quality, and security. This description shall include existing standard test procedures, special-purpose test procedures, test criteria, and experimental design and validation criteria. In the event that this documentation is not available, the Qualification Test agency shall design test cases and procedures equivalent to those ordinarily used as a basis for verification (see below). ***Question: How will this be tested for? Suggestion: This requirement should appear in the CIBER Security Master Test Plan.***

(q) Qualification Test Specification

The vendor shall provide a description of the specification for verification and validation of overall software performance, including acceptance criteria for control and data input/output, processing accuracy, data quality assessment and maintenance, exception handling, and security. The specification shall identify specific procedures by means of which the general suitability of the software for elections use can be assessed and demonstrated. The vendor's specification and procedure shall be used to establish the detailed requirements of the tests described in "Laboratory Environmental Test Procedures for Hardware and Software" of this Standard. ***Question: How will this be tested for? Suggestion: This requirement should appear in the CIBER Security Master Test Plan.***

(r) Acceptance Test Specification

The vendor shall provide a description of the specification for installation, acceptance and readiness verification. This specification shall identify specific procedures by means of which the capability of the software to accommodate actual ballot formats and format logic, and pre-election logic, accuracy and security test requirements of using jurisdictions may be

assessed and demonstrated. The vendor's specification shall be used to establish the detailed requirements of the tests described in "Laboratory Environmental Test Procedures for Hardware and Software" of this standard performed to evaluate the adequacy of the vendor's procedures, and it shall be suitable for inclusion in the regulations and procedures of user counties when preparing for the conduct of actual elections. ***Question: How will this be tested for? Suggestion: This requirement should appear in the CIBER Security Master Test Plan.***

3.2.2 Findings from the Federal VVSG Guidelines

- There should be a section of the Security Master Test Plan that outlines a checklist of security-related requirements for the vendor-supplied TDPs. This plan component should minimally require the check for TDP components as outlined in Section 2.6 of the VVSG Vol 2 2005 Guidelines. ***Suggestion: Include a section to address this.***
- For each requirement stated in the CIBER Security Master Test Plan that maps to a requirement from the 2005 EAC VVSG, the mapping should indicate the specific requirement(s) and not just a general section. ***Suggestion: Provide the specific mapping in all cases.***
- For each requirement that maps to the VVSG, the Test Method and Test Procedures should be described. This description should describe a test method or procedure that is common to all voting machines, so that each machine is tested in a similar fashion; however this will not include machine-specific instructions as those will be addressed in the individual machine test procedures. ***Suggestion: Populate these sections where possible.***
- For many of the VVSG requirements stated in the plan, the TDP and vendor documentation should be stated as sources for compliance checking in addition to "Partial Code Review." ***Suggestion: Reference use of the TDPs where appropriate.***
- Req # 1.8 would imply a test for memory and disk-storage cleansing after use. Is this the intention and if so, how would such an OS feature be tested on a voting machine on which the tester may not have the ability to compile and run a program to test these OS features? ***Suggestion: Clarify and provide specific mapping to VVSG.***
- Req #1.9 may need clarification as to if no network connections are possible and if no non-election software processes are running on the voting machine, then what type of supervisor-type software would monitor the election software processes? ***Suggestion: Clarify and provide specific mapping to VVSG.***
- Req #1.10 would seem to indicate the need for the underlying operating system to be able to assign process priorities. How can this be verified in a partial code review? An alternative test would be to inspect the process

priority of the election software processes and ensure that other processes execute at a lower process priority. This test may require the special system-access abilities. ***Suggestion: Clarify and provide specific mapping to VVSG.***

- Req #1.11 seems to be referring to automated labeling controls. Unsure if this is something that the VVSG requires; please indicate the exact requirement. Also, unsure if a code review will indicate how a system (OS) implements labeling. ***Suggestion: Clarify and provide specific mapping to VVSG.***
- Req #1.19, is this referring to session timeouts for active and inactive sessions? Also, will this test cover voter and administrator-type access timeouts? ***Suggestion: Clarify and provide specific mapping to VVSG.***
- Req #1.24 is referring to label-based controls as defined in the NIST SP800-53 document and does not appear to match up to a corresponding VVSG requirement. Will this be required of voting machines, and is it applicable as this type of requirement is generally applied to systems that implement mandatory data classification and marking requirements? ***Suggestion: Clarify and provide specific mapping to VVSG.***
- Req # 2.16, is this referring to data retention, encryption of removable media, or physical tamper-evident controls. ***Suggestion: Clarify and provide specific mapping to VVSG.***
- Req # 2.18 as written would likely fail many machines. Many machines have modem jacks and PCMCIA slots. If there is no mapping on this requirement, can we hold a machine/vendor to it? ***Suggestion: Clarify and provide specific mapping to NYS requirement.***
- Req #3.13 is right out of the NIST SP800-53 document, but does not seem to be part of the VVSG requirements. ***Suggestion: Clarify and provide specific mapping to NYS requirement.***
- On requirement #3.15, the test plan should indicate which audit record or records (voter audit records, system administrator audit access etc.) the requirement is referring.. ***Suggestion: Clarify***
- Req #3.22 should more clearly define security violations and distinguish between those violations that cause the machine to stop functioning during an election as per section 2.1.3 of VVSG Vol 1. ***Suggestion: Clarify and provide specific mapping to VVSG.***
- Req #3.37 should read that all implementations of FIPS-140-compliant encryption modules should be evaluated for proper implementation. If there is cryptographic software in the code base, but it is not used, will it be checked or cause a machine to fail? ***Suggestion: Clarify.***

- The Security Master Plan should provide a high-level description of testing procedures and plans for machine compliance with Section 7 of the VVSG Vol 1 2005 Guidelines.
- Req #3.38 needs clarification on which records will require a digital signature in NYS.
- Include a requirement to provide documentation of mandatory administrative procedures for effective system security.

3.2.3 Findings from the NYS 2006 Election Law

- Requirement 4.5 needs to say that the network devices do not exist or that they exist and could potentially be used. NYS Law states: "not include any device or functionality potentially capable of externally transmitting or receiving data via the internet or via radio waves or via other wireless means."