

**New York State Voting Project
Security Verification Testing**

**Security Requirements Test Matrix
Draft Until Reviewed**

September 6, 2006

Prepared For:

New York State Board of Elections (BOE)

Submitted By:

CIBER Global Security Practice
5251 DTC Parkway, Suite 600
Greenwood Village, Colorado 80111
www.ciber.com

TABLE OF CONTENTS

REVISION HISTORY	3
INTRODUCTION	4
BACKGROUND	4
New York State	4
CIBER's Global Security Practice.....	4
OVERVIEW AND APPROACH	4
SECURITY TASK EXCLUSIONS	6
NEW YORK STATE VOTING SECURITY TEST REQUIREMENTS MATRIX	7
SELECTION OF TEST METHODS	7
ACCESS CONTROL SECURITY REQUIREMENTS	10
PHYSICAL SECURITY REQUIREMENTS	17
SOFTWARE SECURITY REQUIREMENTS	23
TELECOMMUNICATIONS AND DATA TRANSMISSION SECURITY REQUIREMENTS	46
USE OF PUBLIC COMMUNICATIONS NETWORKS SECURITY REQUIREMENTS	49
WIRELESS COMMUNICATIONS SECURITY REQUIREMENTS	50

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

REVISION HISTORY

Date	Version	Description	Author
09/06/2006	V1.0	Document Creation	Carolyn Ryll, CISSP CIBER's Global Security Practice
09/08/2006	V2.0	Change to different documents template; document marked "Draft"	Carolyn Ryll, CISSP CIBER's Global Security Practice
09/09/2006	V3.0	Modification of security testing methods to NIST 800-53A from CIBER methodology	Carolyn Ryll, CISSP CIBER's Global Security Practice
09/14/2006	V3.1	Modification of introductory sections	Carolyn Ryll, CISSP CIBER's Global Security Practice

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

INTRODUCTION

BACKGROUND

New York State

Before voting equipment may be sold in New York State (NYS), it must be examined by the New York State Board of Elections (NYSBOE). The examination shall include a thorough review and testing of all electronic and computerized security features on a voting system. The contractor CIBER will work closely with the staff of the NYSBOE in all phases of the examination. In executing this work, CIBER will also be required to interact with the New York State Technology Enterprise Corporation (NYSTEC) who has been contracted by NYSBOE to perform certain independent oversight functions related to planning and execution of the voting equipment tests.

CIBER's Global Security Practice

CIBER's Global Security Practice focuses exclusively on information security. Our professional staff designs, implements, and manages security solutions for critical information systems in a wide range of commercial and Federal environments. Since 1992, organizations desiring superior security engineering and consulting services have turned to CIBER Security to fulfill their information security needs.

OVERVIEW AND APPROACH

The CIBER Security and NYSTEC teams are tasked with performing a combination of testing and analysis of thirteen different vendor-supplied voting systems to verify security of the controls. The testing is structured to identify and evaluate as much potential vulnerability or compliance as is feasible within a reasonable level of effort.

The CIBER Security approach to this engagement is comprised of three phases designed to provide a comprehensive, yet cost-effective evaluation of the voting systems' technical security posture:

- 1. Security Test Planning**

During this phase, a comprehensive security test plan is developed against the NY State

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

requirements, Voluntary Voting System Guidelines, guidelines of the Help America Vote Act (HAVA), 2006 NY Election Law, NIST 800-37 “Guide for the Security Certification and Accreditation of Federal Information Systems”, NIST 800-53 “Recommended Security Controls for Federal Information Systems”, and NIST 800-53A “Guide for Assessing the Security Controls in Federal Information Systems. This test plan is located within this document. This includes system familiarization, creation of a security requirements traceability matrix, selection of test methods, and development of test scripts. Definition of the test schedule and identification of prerequisites for testing activities also occurs in this phase.

2. Security Testing

During this phase, the presence and effectiveness of technical and non-technical security controls of the systems are verified against the above-mentioned requirements and guidelines to ensure that system requirements are satisfied and that the system provides the desired level of assurance. This involves executing each of the tests listed in this document and recording the results.

3. Security Test Reporting

During this phase, a report is prepared that covers all security testing results. The basis of the report will be that which is contained in this document that includes testing results (Compliant, Partially Compliant, or Non-Compliant) for each of the requirements tested. The report will contain a text summary of all testing, test plans, test results and analysis, and a detailed review of non-test (e.g., demonstrations, observations, inspections/examinations) activities. Attachments will be added as necessary for technical and amplifying data.

Where security is verified throughout this report, the font color has been adjusted to give easy understanding of the compliance or noncompliance of each one. Where the font is **blue** demonstrates an item that does not necessarily denote a lack of compliance, but an informational item or a focal point where security could be heightened in selected circumstances. Where the font is **green** demonstrates full compliance to security industry best practices and shows where a voting system is successful in its approach. Where the font is **yellow** demonstrates partial compliance that may demonstrate a mild level of risk. Where the font is **orange** shows a partial compliance, in which vulnerabilities should be mitigated in a timely manner, as risk levels increase at this point. **Red** demonstrates high vulnerabilities and noncompliance that requires further analysis by the business and strong recommendation to mitigate by CIBER Security and NYSTEC. Where it is **dark red** represents critical vulnerabilities and noncompliance that need to be addressed right away.

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

The scoring of each system's compliance with individual security requirements will be rated Pass, Partial, Fail, or Not Applicable (N/A) as applicable. When a security system feature is not present where it could be used to enhance the security of the device, or where adding the additional security feature would have no positive effect on the security of the system, the element will be given the rating "N/A".

SECURITY TASK EXCLUSIONS

For purposes of evaluating a voting system that is provided by a vendor, certain elements of security are not under control of the vendor and shall not be addressed in this security testing specification.

Per Volume I of the 2005 Voluntary Voting System Guidelines, section 7.1.1 "Elements of Security Outside Vendor Control", these practices include:

- Administrative and management controls for the voting system and election management – including access controls (Note: For purposes of this specification, we will refer to this access control as "physical access control" and not as access control that allows or denies functionality of the system as provided by the vendor.)
- Internal security procedures
- Adherence to, and enforcement of, operational procedures (e.g., effective password management)
- Security of physical facilities
- Organizational responsibilities and personnel screening

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

NEW YORK STATE VOTING SECURITY TEST REQUIREMENTS MATRIX

SELECTION OF TEST METHODS

For each item in this matrix, CIBER Security and NYSTEC evaluate the available testing techniques to select the most effective method or methods for each item. Test methods per NIST Special Publication 800-53A “Guide for Assessing the Security Controls of Federal Information Systems” are defined as:

- **Interview**

The interview method of assessment is the process of conducting focused discussions with individuals or groups of individuals within an organization to facilitate assessor understanding, achieve clarification, or obtain evidence. Assessment objects are individuals or groups of individuals. Attributes are Depth and Coverage (see below for more on Attributes).

- The Interview *Depth* Attribute addresses the rigor and level of detail in the interview process, for which there are three possible value: Generalized, Focused, and Comprehensive.
 - Generalized interviews consist of broad, high-level discussions with selected organizational personnel on particular topics relating to the security controls being assessed. This is typically conducted using a set of generalized, high-level questions and is intended to capture a broad, general understanding of the fundamental concepts associated with specifications, mechanisms, or activities.
 - Focused interviews consist of broad, high-level discussions and more detailed discussions in specific areas with selected organizational personnel on particular topics relating to the security controls being assessed. This is typically conducted using a set of generalized, high-level questions and a set of more detailed questions in specific areas where responses indicate a need for more detailed investigation and is intended to capture the specific understanding of the fundamental concepts associated with specifications, mechanisms, or activities.
 - Comprehensive interviews consist of broad, high-level discussions and more detailed, probing discussions in specific areas with selected organizational personnel on particular topics relating to the security controls being assessed (including the results of other assessment methods). This is typically conducted using a set of generalized, high-level

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

questions and a set of more detailed, probing questions in specific areas where response indicate a need for more detailed investigation or where assessment evidence allows and is intended to capture the specific understanding of the fundamental concepts and implementation details associated with specifications, mechanisms, or activities.

- The Interview *Coverage* Attribute addresses the categories of individuals to be interviewed (by organizational roles and responsibilities) and the number of individuals to be interviewed (by category).

- **Examine**

The examine method of assessment is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (I.e., specifications, mechanisms, or activities). Similar to the interview method, the primary purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence. Assessment objects are Specifications (e.g., policies, plans, procedures, system requirements, designs); Mechanisms (e.g., hardware, software, firmware); and Activities (e.g., system operations/administration/management, exercises, drills). Attributes are Depth and Coverage.

- The Examine *Depth* Attribute addresses the rigor and level of detail in the examination process, for which there are three possible values: Generalized; Focused; and Comprehensive.
 - Generalized examinations consist of brief, high-level reviews, observations, or inspections of security controls using a limited body of evidence or documentation. These are typically conducted using functional-level descriptions of specifications, mechanisms, or activities.
 - Focused examinations consist of detailed analyses of security controls using a substantial body of evidence or documentation. These types of examinations are typically conducted using functional-level descriptions of specification, mechanisms, or activities, and where appropriate, high-level design information.
 - Comprehensive examinations consist of detailed and thorough analyses of security controls using an extensive body of evidence or documentation. These are typically conducted using functional-level descriptions of specifications, mechanisms, or activities,

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

and where appropriate, high-level design, low-level design, and implementation-related information (e.g., source code).

- The Examine *Coverage* Attribute addresses the categories of specifications, mechanisms, or activities to be examined and the number of specifications, mechanisms, or activities to be examined (by category).
- **Test**

The test method of assessment is the process of exercising one or more assessment objects (limited to activities or mechanisms) under specified conditions to compare actual with expected behavior. Assessment objects are Mechanisms (e.g., hardware, software, firmware); and Activities (e.g., system operations/administration/management, exercise, drills).
- The Test *Type* Attribute addresses the types of testing to be conducted, for which there are three possible values: Functional testing, Penetration testing; and Structural testing.
 - Functional Testing is a test methodology that assumes knowledge of the functional specifications, high-level design, and operating specifications of the item under assessment (also known as “black box” testing).
 - Penetration Testing is a test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.
 - Structural Testing is a test methodology that assumes (some) explicit knowledge of the internal structure of the item under assessment (e.g., low-level design, source code implementation representation). (Also known as “gray box” or “white box” testing.)
- The Test *Coverage* Attribute addresses the categories of mechanisms or activities to be tested and the number of mechanisms or activities to be tested (by category). For mechanism-related testing that involves software, the coverage attribute also addresses the extent of the testing conducted (e.g., number of test cases, number of modules tested, etc.)

In all three cases (I.e., interview, examine, and test) where the assessment methods are employed, the results are used to support the determination of overall security control effectiveness.

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

The assessment method attributes and attribute values will test by the following information system impact level:

- The security control is in effect and meets explicitly identified functional requirements in the control statement. The focus is on ensuring correct implementation and operation of the control. Comprehensive interviews and examinations are conducted. Functional, structural, and penetration testing are employed to ensure that there are no obvious errors in the security control, that the security control is implemented correctly, and operating as intended.

ACCESS CONTROL SECURITY REQUIREMENTS			
These standards address procedures and system capabilities that limit or detect access to critical system components in order to guard against loss of system integrity, availability, confidentiality, and accountability. This is limited to those controls required to be provided by system vendors, and may be divided into four focus areas: General Access Control Policy; Individual Access Privileges; Access Control Measures, and Other Considerations.			
Req #	1.1	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system separates user functionality (including user interface services) from system management functionality.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>
Req #	1.2	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-3	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system isolates security functions from non-security functions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>
Req #	1.3	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-3(1)	Test Procedures	<i>State procedures used to test for this requirement</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Requirement Description	The system employs underlying hardware separation mechanisms to facilitate security function isolation.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.4	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-3(2)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system isolates critical security functions (I.e., functions enforcing access and information flow control) from both non-security functions and from other security functions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>
Req #	1.5	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-3(3)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system minimizes the number of non-security functions included within the isolation boundary containing security functions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>
Req #	1.6	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-3(4)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system maintains its security functions in largely independent modules that avoid unnecessary interactions between modules.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Req #	1.7	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-3(5)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system security maintains its security functions in a layered structure minimizing interactions between layers of the design.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>
Req #	1.8	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-4	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system prevents unauthorized and unintended information transfer via shared system resources.	Actual Results	
Documented Dependencies		Additional Notes	<i>Control of information system remnants, sometimes referred to as object reuse, prevents information, including encrypted representations of information, produced by the actions of a prior user/role from being available to any current user/role (or current process) that obtains access to a shared system resource after that resource has been released back to the system.</i>
Req #	1.9	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-5(2)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial of service attacks.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.10	Test Method	<i>State methods used to test for this requirement</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-6	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system limits the use of resources by priority.	Actual Results	
Documented Dependencies		Additional Notes	<i>Priority protection ensures that a lower-priority process is not able to interfere with the information system servicing any higher-priority process.</i> <i>Partial Code Review</i>
Req #	1.11	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-16	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system appropriately labels information in storage, in process, and in transmission.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>
Req #	1.12	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-5	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system enforces separation of duties through assigned access authorizations.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.13	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-6	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Documented Dependencies		Additional Notes	
Req #	1.14	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 IA-2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system uniquely identifies and authenticates users (or processes acting on behalf of users).	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.15	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 IA-3	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system identifies and authenticates specific devices before establishing a connection.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.16	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.17	Test Method	<i>State methods used to test for this requirement</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 SC-14	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	For publicly available information and applications, the system protects the integrity and availability of the information and applications.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.18	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Each person to whom access is granted is identified by the system, along with the specific functions and data to which each person holds authorized access.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.19	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-12	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	An individual's authorization is limited to a specific time, time interval, or phase of the voting or counting operations.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.20	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The voter is permitted to cast a ballot expeditiously, but preclude voter access to all aspects of the vote counting processes.	Actual Results	
Documented Dependencies		Additional Notes	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Req #	1.21	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-3	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system enforces assigned authorizations for controlling access to the system.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.22	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-3(1)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system ensures that access to security functions (deployed in hardware, software, and firmware) and security-relevant information is restricted to explicitly authorized personnel (e.g., security administrators, system administrators, and other privileged users).	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.23	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-4	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	1.24	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-4(1)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement	Label-based control: Flow control enforcement uses	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Description	explicit labels on information, source, and destination objects as a basis for flow control decisions (e.g., to control the release of certain types of information).		
Documented Dependencies		Additional Notes	
Req #	1.25	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 AC-4(2)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Domain-based control: Flow control enforcement uses protected processing domains (e.g., type-enforcement) as a basis for flow control decisions.	Actual Results	
Documented Dependencies		Additional Notes	
<End of New York State Voting Access Control Security Requirements>			

PHYSICAL SECURITY REQUIREMENTS

These standards address physical security measures and procedures that prevent disruption of the voting process at the polling place and corruption of voting data, as well as considerations toward other forms of physically affecting the system. This may be divided into three focus areas: Polling Place Security; Central Count Location Security, and Other Considerations.

Req #	2.1	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Detailed documentation exists containing measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Req #	2.2	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Documented measures demonstrate how to immediately detect tampering with vote casting devices and precinct ballot counters.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	
Req #	2.3	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Documented measures demonstrate how to control physical access to a telecommunications link, if such a link is provided.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	
Req #	2.4	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Documented measures to enable poll workers to physically protect and perform orderly shutdown of voting equipment to counteract vandalism, civil disobedience, and similar occurrences work as specified.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	
Req #	2.5	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement	Documented measures that demonstrate how to	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Description	immediately detect tampering with vote casting devices and precinct ballot counters work as specified.		
Documented Dependencies	Vendor documentation	Additional Notes	
Req #	2.6	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Documented measures that demonstrate how to control physical access to a telecommunications link, if such a link is provided, work as specified.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	
Req #	2.7	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Documentation details measures to be taken in a central counting environment, to include physical and procedural controls related to the handling of ballot boxes, preparing of ballots for counting, counting operations and reporting data.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	
Req #	2.8	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Safeguards are present to protect against tampering during system repair or interventions in system operations.	Actual Results	
Documented Dependencies		Additional Notes	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Req #	2.9	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Safeguards effectively protect against tampering during system repair or interventions in system operations.	Actual Results	
Documented Dependencies		Additional Notes	<i>This varies from the preceding requirement in that the former states controls are present; this requirement states that they work.</i>
Req #	2.10	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	If the voting system tabulates ballots through provision of a counter, controls are in place to prevent the resetting of the counter except by authorized individuals.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	2.11	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	If the voting system tabulates ballots through provision of a counter, controls are effective in the prevention of resetting the counter except by authorized individuals.	Actual Results	
Documented Dependencies		Additional Notes	<i>This varies from the preceding requirement in that the former states controls are present; this requirement states that they work.</i>
Req #	2.12	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			<i>requirement</i>
Requirement Description	If the voting system tabulates ballots through provision of a counter, controls are in place to prevent the increase of count except by the input of a ballot.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	2.13	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	If the voting system tabulates ballots through provision of a counter, controls are effective in the prevention of the increase of count except by the input of a ballot.	Actual Results	
Documented Dependencies		Additional Notes	<i>This varies from the preceding requirement in that the former states controls are present; this requirement states that they work.</i>
Req #	2.14	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 3 and 4	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The audio interface disallows the ability to capture sound emissions through means of a foreign device.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	2.15	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 3 and 4	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The audio interface disallows the ability to capture electronic emissions through means of a foreign device.	Actual Results	
Documented		Additional Notes	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Dependencies			
Req #	2.16	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 4	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Memory devices demonstrate resistance to tampering.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	2.17	Test Method	<i>State methods used to test for this requirement</i>
Mapping	VVSG Volume 1 Section 4	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Removable storage media (magnetic media, optical media, etc.) demonstrates resistance to tampering.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	2.18	Test Method	<i>State methods used to test for this requirement</i>
Mapping	N/A	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Capacity to attach a foreign, undocumented device to the system does not exist.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	2.19	Test Method	<i>State methods used to test for this requirement</i>
Mapping	N/A	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Voting system security seals and device locks are present to guard against access to machine panels, doors, switches, slots, ports, peripheral devices, firmware, and software.	Actual Results	
Documented		Additional Notes	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Dependencies			
Req #	2.20	Test Method	<i>State methods used to test for this requirement</i>
Mapping	New York State Voting Requirements; 2006 NY Election Law	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Voting system security seals and device locks are effective in their guard against access to machine panels, doors, switches, slots, ports, peripheral devices, firmware, and software.	Actual Results	
Documented Dependencies		Additional Notes	<i>This varies from the preceding requirement in that the former states controls are present; this requirement states that they work.</i>
Req #	2.21	Test Method	<i>State methods used to test for this requirement</i>
Mapping	2006 NY Election Law	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The voting system secures any votes already cast on the system during multiple forms of malfunctioning.	Actual Results	
Documented Dependencies		Additional Notes	<i>This requirement is encouraged to be approached cautiously during the testing cycle, with consideration made to testing of this requirement toward the end of the test phase. Should attempts to cause a malfunctioning system place the system in an unrecoverable state, unexpected delays in the testing cycle may occur.</i>
<End of New York State Voting Physical Security Requirements>			

SOFTWARE SECURITY REQUIREMENTS

These standards address the installation of software, including firmware, in the voting system and the protection against malicious software. It should be noted that computer-generated audit controls facilitate system security and are an integral part of software capability. This may be divided into three focus

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

areas: Software and Firmware Installation; Protection Against Malicious Software*: and Other Considerations.

***Note:** "Protection Against Malicious Software" takes into account Section 6209.2 Polling Place Voting System Requirements "G" of Subtitle V of Title 9 of the Official Compilation Codes, Rules and Regulations of the State of New York, which states "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." This is to include a review of Application Vulnerability as well as Application Code.

Req #	3.1	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Vendor documentation states that every device is to be retested to validate each ROM prior to the start of elections operations.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	<i>This requirement is specific to those systems in which software is resident in the system as firmware.</i>
Req #	3.2	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	For any software permanently installed or resident in the voting system, vendor system documentation states that the jurisdiction must provide a secure physical and procedural environment for the storage, handling, preparation, and transportation of the system hardware.	Actual Results	
Documented Dependencies	Vendor system documentation	Additional Notes	
Req #	3.3	Test Method	<i>State methods used to test for this requirement</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			<i>as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Any voting system bootstrap, monitor, and device-controller software that is resident permanently as firmware is inaccessible to activation or control by any means other than by the authorized initiation and execution of the vote counting program, and its associated exception handlers.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.4	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Election-specific programming that is installed and resident as firmware is installed on a component (such as a computer chip) other than the component on which the operating system resides.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.5	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	After initiation of election day testing, no source code or compilers or assemblers are resident or accessible.	Actual Results	
Documented		Additional Notes	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Dependencies			
Req #	3.6	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	System protection is present to defend against file and macro viruses, worms, Trojan horses, and logic bombs.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.7	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Procedures to maintain adequate protection against file and macro viruses, worms, Trojan horses, and logic bombs are provided in vendor documentation.	Actual Results	
Documented Dependencies	Vendor documentation	Additional Notes	
Req #	3.8	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; HAVA 2002	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides for the capability to create and maintain a real-time audit record.	Actual Results	
Documented Dependencies		Additional Notes	<i>This capability records and provides the operator or precinct official with continuous</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			<i>updates on machine status. This information allows effective operator identification of an error condition requiring intervention, and contributes to the reconstruction of election-related events necessary for recounts or litigation.</i>
Req #	3.9	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53 AU-8(1)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system maintains an absolute record of the time and date or a record relative to some event whose time and date are known and recorded.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.10	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53 AU-8	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	All audit record entries include the time-and-date stamp.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.11	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement	The audit record is active whenever the system is in	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Description	an operating mode and is available at all times.		
Documented Dependencies		Additional Notes	<i>The audit record need not be continually visible while active.</i>
Req #	3.12	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53-rev1 AU-9	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The generation of audit record entries cannot be terminated or altered by program control, or by the intervention of any person. The system protects audit information and audit tools from unauthorized access, modification, and deletion.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.13	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53-rev1 AU-9(1)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system produces audit information on hardware-enforced, write-once media.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.14	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system preserves the contents of the audit record during any interruption of power to the	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

	system until processing and data reporting have been completed.		
Documented Dependencies		Additional Notes	
Req #	3.15	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system is capable of printing a copy of the audit record.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.16	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53-rev1 AU2(1)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides the capability to compile audit records from multiple components throughout the system into a system-wide (logical or physical), time-correlated audit trail.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.17	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53-rev1 AU3(1)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides the capability to include additional, more detailed information in the audit	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

	records for audit events identified by type, location, or subject..		
Documented Dependencies		Additional Notes	
Req #	3.18	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53-rev1 AU3	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Audit records produced by or associated with the system contain sufficient information to establish what events occurred, the sources of events, and the outcomes of the events.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.19	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53-rev1 AU-5(1)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides a warning when allocated audit storage volume reaches maximum storage capacity.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.20	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 2; NIST SP800-53-rev1 AU-5(2)	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides a real-time alert when audit failure events occur.	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Documented Dependencies		Additional Notes	
Req #	3.21	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	N/A	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	Error messages are generated for security violations.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.22	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	NIST SP800-53 SI-11	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system identifies and handles error conditions in an expeditious manner.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.23	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 5	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system does not contain software for any other purpose than that related to voting efforts.	Actual Results	
Documented Dependencies		Additional Notes	<i>Some voting systems use computers that also may be used for other purposes, containing general purpose software such operating systems, programming language compilers,</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			<i>database management systems, and Web browsers.</i>
Req #	3.24	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 5; VVSG Volume 2 Section 5	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system's development environment provides controls to prevent accidental or deliberate attempts to replace executable code through unbounded arrays or strings (includes buffers used to move data); Pointer variables; Dynamic memory allocation and management.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.25	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software provides methods or capabilities for detecting and handling exception conditions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.26	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement	The system software provides methods or	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Description	capabilities for detecting and handling system failures.		
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.27	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software provides methods or capabilities for detecting and handling data input/output errors.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.28	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 2	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software provides security error logging for audit record generation.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.29	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 2; NIST SP800-53-rev1 SI-7	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software provides methods or capabilities for security monitoring and control.	Actual Results	
Documented		Additional Notes	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Dependencies			
Req #	3.30	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 2; NIST SP800-53-rev1 SI-6	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system verifies the correct operation of security functions upon system startup and restart and upon command by user with appropriate privilege and notifies the administrator when anomalies are discovered.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.31	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 2; VVSG Volume 2 Section 5; NIST SP800-53-rev1 SI-10	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software provides methods or capabilities for assessing data quality. (Input data should be validated for correctness. All parameters are validated for type and range on entry into each unit.)	Actual Results	
Documented Dependencies		Additional Notes	<i>The system should check information for accuracy, completeness, validity, and authenticity.</i> <i>Code Review</i>
Req #	3.32	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Mapping	VVSG Volume 2 Section 5	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software provides controls to prevent writing beyond arrays, strings, or buffer boundaries.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.33	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 5	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software provides controls that prevent a pointer or address from being used to overwrite executable instructions or to access inappropriate areas where vote counts or audit records are stored.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.34	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 2 Section 5	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system software prevents any vote counter from overflowing.	Actual Results	
Documented Dependencies		Additional Notes	<i>Assumption that the counter size is large enough such that the value will never be reached is not sufficient.</i> <i>Code Review</i>
Req #	3.35	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			Methods
Mapping	NY State Requirements	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	All cryptographic software in the voting system has been approved by the U.S. Government's Crypto Module Validation Program (CMVP).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.36	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	VVSG Volume 1 Section 7; NIST SP800-53-rev1 IA-7; NIST SP800-53-rev1 SC-13	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	For authentication to a cryptographic module, the system employs authentication that meets the requirements of FIPS 140-2 (as amended).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.37	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	All cryptographic software in the voting system has been implemented correctly.	Actual Results	
Documented Dependencies		Additional Notes	<i>Partial Code Review</i>
Req #	3.38	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Mapping	NY State Requirements	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The voting system generates and stores a digital signature for each electronic record.	Actual Results	
Documented Dependencies		Additional Notes	
Req #	3.38	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	NY State Requirements	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The voting system's software does not contain any code, procedures, or other material that 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.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.39	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not contain unbounded string copies nor allow for out-of-bounds writing.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Req #	3.40	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	All allocated memory is freed when no longer in needed.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.41	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not contain (or guards against) off-by-one errors.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.42	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not contain null-termination errors.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.43	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code allots enough space in destination character arrays to hold the contents of a string (I.e., guard from vulnerability by string truncation).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.44	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against buffer overflows.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i> <i>Buffer overflows may result from null-termination issues; lack of implicit bounds checking; or standard string library calls that do not enforce bounds checking.</i>
Req #	3.45	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code provides error or exception handling for special cases of exceptions (such as divide-by-zero) as well as unexpected program termination.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Req #	3.46	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code chains exception handlers, calling in a defined order until one can handle the exception.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.47	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against initialization errors (failure to initialize parameters or blocks of memory).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.48	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not fail to check return values (I.e., ensuring that memory allocation routines succeeded, etc.).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.49	Test Method	<i>State methods used to test for this requirement</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			<i>as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not reference freed memory.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.50	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not free the same memory multiple times.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.51	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not improperly pair memory management functions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.52	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Requirement Description	The system code does not fail to distinguish between scalars and arrays (I.e., new and delete for scalars; new[] and delete[] for arrays).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.53	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not make improper use of allocation functions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.54	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not write to memory that has already been freed.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.55	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code applies appropriate integer range checking for the given type.	Actual Results	
Documented		Additional Notes	<i>Code Review</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Dependencies			
Req #	3.56	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code applies integer promotions appropriately.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.57	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code makes appropriate use of integer conversions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.58	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against integer overflow.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.59	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			Methods
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against sign errors (I.e., converting a signed integer to an unsigned integer).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.60	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against truncation errors (I.e., converting an integer to a small integer type and the value of the original is outside the range of the smaller.)	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.61	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code identifies all data input sources (I.e., command line variables, environmental variables, etc.).	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.62	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code sanitizes all input data.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.63	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against race conditions.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.64	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against temporary-file-open exploits.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.65	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code does not trust filenames without adequate verification.	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Documented Dependencies		Additional Notes	<i>Code Review</i>
Req #	3.66	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	CIBER Security: Secure Coding Practices	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system code guards against format string vulnerabilities.	Actual Results	
Documented Dependencies		Additional Notes	<i>Code Review</i> <i>Format string vulnerabilities can occur when a format string (or portion of a string) is supplied by a user or other untrusted source.</i>
<End of New York State Voting Software Security Requirements>			

TELECOMMUNICATIONS AND DATA TRANSMISSION SECURITY REQUIREMENTS

These standards address security for the electronic transmission of data between system components or locations over private, public, and wireless networks. This may be divided into five sections: Data Integrity; Protection Against External Threats; Capability to Monitor and Respond to External Threats; Shared Operating Environment; and Provision for Incomplete Election Returns.

Note: These requirements need only be tested to demonstrate a system's capacity to not provide networking capability over private, public, or wireless networks.

Req #	4.1	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement	The system does not provide for the electronic	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Description	transmission of data between system components over networks.		
Documented Dependencies	Vendor documentation should explicitly state that they system does not provide for this functionality.	Additional Notes	
Req #	4.2	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system does not provide for the electronic transmission of data between locations over private networks.	Actual Results	
Documented Dependencies	Vendor documentation should explicitly state that they system does not provide for this functionality.	Additional Notes	
Req #	4.3	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system does not provide for the electronic transmission of data between locations over public networks.	Actual Results	
Documented Dependencies	Vendor documentation should explicitly state that they system does not provide for this functionality.	Additional Notes	
Req #	4.4	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system does not provide for the electronic transmission of data between locations over wireless	Actual Results	

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

	networks.		
Documented Dependencies	Vendor documentation should explicitly state that they system does not provide for this functionality.	Additional Notes	
Req #	4.5	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides for the electronic transmission of data between system components over networks, but provides for the capacity to disable this functionality.	Actual Results	
Documented Dependencies	Vendor documentation should give explicit directions on how to disable this functionality along with predicted side effects on system behavior once this functionality is disabled.	Additional Notes	
Req #	4.6	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides for the electronic transmission of data between locations over private networks, but provides for the capacity to disable this functionality.	Actual Results	
Documented Dependencies	Vendor documentation should give explicit directions on how to disable this functionality along with predicted side effects on system behavior once this functionality is disabled.	Additional Notes	
Req #	4.7	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test</i>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

			<i>Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides for the electronic transmission of data between locations over public networks, but provides for the capacity to disable this functionality.	Actual Results	
Documented Dependencies	Vendor documentation should give explicit directions on how to disable this functionality along with predicted side effects on system behavior once this functionality is disabled.	Additional Notes	
Req #	4.8	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping		Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system provides for the electronic transmission of data between locations over wireless networks, but provides for the capacity to disable this functionality.	Actual Results	
Documented Dependencies	Vendor documentation should give explicit directions on how to disable this functionality along with predicted side effects on system behavior once this functionality is disabled.	Additional Notes	
<End of New York State Voting Telecommunications and Data Transmission Security Requirements>			

USE OF PUBLIC COMMUNICATIONS NETWORKS SECURITY REQUIREMENTS

These standards address security for systems that communicate individual votes or vote totals over public communications networks. This may be divided into two sections: Data Transmission; and Casting Individual Ballots (for systems designed for transmission of telecommunications over public networks).

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.

Note: Please refer to [“Telecommunications and Data Transmission Security Requirements”](#)

N/A

<End of New York State Voting Use of Public Communications Networks Security Requirements>

WIRELESS COMMUNICATIONS SECURITY REQUIREMENTS

These standards address the security of the voting system and voting data when wireless is used.

Note: Please refer to [“Telecommunications and Data Transmission Security Requirements”](#)

Req #	6.1	Test Method	<i>State methods used to test for this requirement as defined in the section Selection of Test Methods</i>
Mapping	2006 NY Election Law – 7-202	Test Procedures	<i>State procedures used to test for this requirement</i>
Requirement Description	The system does not include any device or functionality capable of externally transmitting or receiving data via the Internet, radio waves, or other wireless means.	Actual Results	
Documented Dependencies		Additional Notes	

<End of New York State Voting Wireless Communications Security Requirements>

USE AND DISCLOSURE OF INFORMATION IN THIS DOCUMENT

This document contains information and reporting methodologies that are confidential and proprietary to NYS BOE and/or the CIBER Global Security Practice. The document and the information contained within it and its attachment(s) as applicable may be used by the intended recipient only. All information remains the property of CIBER and NYS BOE and any other use or disclosure of this information requires prior written approval. © 2006, CIBER, Inc.