Your Independent Technology Advisor

Independent Review of SysTest Certification Security Test Findings

Submitted to:

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

December 11, 2009
Version 1.2 - Draft

Table of Contents

1. INDEPENDENT REVIEW OF SECURITY CERTIFICATION TEST FINDINGS SUMMARY

1.1 Executive Summary and NYSTEC recommendation

This report presents NYSTEC's review of SysTest Lab's certification test findings for the Dominion and ES&S Electronic Voting Systems proposed for use in New York State (NYS). This report also presents considerations for compensating controls to address findings and permit the use of the Dominion and ES&S Electronic Voting Systems in a manner that assures the security and integrity of the voting process in New York State.

NYSTEC's central task was to determine, based on the SysTest findings, if the tested systems can be used in a way that assures the security and integrity of the voting process. Based on NYSTEC's independent review of the test findings, NYSTEC believes that both systems can be used for elections in New York, provided appropriate controls are put in place to compensate for potential security risks resulting from test findings. Compensating controls will be discussed in detail later in this report.

NYSTEC has considered the findings from SysTest's testing, together with its knowledge of voting systems, NYS Election environment, and security best practices to develop recommendations regarding the appropriate use of the electronic voting systems in a manner that mitigates potential security risks. The compensating controls recommended by NYSTEC build upon existing New York State Board of Election (NYSBOE) Policies and Procedures and will require NYSBOE and the County Board of Elections (CBOE) to create and follow much more stringent procedures for working with the voting systems. On the Functional Testing side, for all negative findings, SysTest and NYSBOE are identifying compensating controls, or workarounds, that would allow the voting systems to be safely used for elections. NYSTEC believes that both vendor systems can be used in a safe and secure manner in NYS when all identified compensating controls are in place.

Implementing the identified compensating controls will be necessary for the safe use of these systems. NYSTEC recommends that NYSBOE Policies and Procedures be re-examined and revised to incorporate all compensating controls identified and to reflect findings from certification testing and the statewide pilot. Once these procedures are properly documented and successfully implemented, NYSTEC is confident risks resulting from test findings are sufficiently mitigated and will enable these systems to be used safely used for NY elections.

1.2 NYSTEC Certification Testing Observations

NYSTEC offers the following observations about the NYSBOE voting system selection and Certification testing process:

- NYSTEC believes that the NY State Certification testing of these systems has been more extensive than testing efforts executed for other voting systems that have received Election Assistance Commission (EAC) certification.
- The systems submitted are optical scan paper ballot systems which represent an important step and commitment to election transparency and security. These systems have an inherent property known as Software Independence. "Software independence" means

that an undetected error or fault in the voting system's software is not capable of causing an undetectable change in election results."[1] This is an important property in the evaluation of the security of the Dominion and ES&S paper ballot systems because it permits transparent and trusted elections, even in the event of a software failure.

- There were many valid findings identified throughout the overall testing effort (two years) and many break fix cycles between the vendors, SysTest, NYSBOE, and NYSTEC that resulted in significant improvements in the functionality and security of each system. Vendors responded to these findings by improving their respective systems. Some of the areas where improvements were seen include:
    - Physical Security features of both systems were improved through vendor modifications to system design that better allow for the use of protective locks and seals and permit improved voter privacy.
    - Improvements to vendor documentation occurred throughout the process.
    - Both vendors made progress in the security of their systems by implementing cryptographic controls such as encryption to provide confidentiality and digital signatures (and other techniques) to provide integrity to the voting process.
    - Improvements in the implementation of access controls and auditing on the Election Management Systems.
- The testing results identified where security features were implemented well and where there was a need for compensating controls.
- The cryptographic source code review performed by the SysTest subcontractor (Cigital) was comprehensive and identified the degree to which each vendor was Federal Information Processing Standards (FIPS) 140-2 compliant with their respective implementations of cryptographic functions.
- Negative testing was done selectively throughout the security test cases to test the effectiveness of the voting system security features. Negative testing involves tests that attempt to circumvent security features to ascertain if the controls are effective. In other words, regular testing is done to see if the system works per the requirements, and negative testing is done to see how the system fails.
- Identification and awareness of potential vulnerabilities and system problems provides an opportunity to proactively address these issues. When potential issues regarding security and functionality are identified, NYSTEC can then recommend compensating controls to mitigate these risks. Certification testing was successful in this area.

[1] Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission, August 31, 2007,

2. BACKGROUND

The NYSBOE has asked NYSTEC to conduct an independent review of the security test findings by SysTest Labs for the New York State Electronic Voting System Certification Project.

NYSTEC has assisted NYSBOE during the testing process over the course of the last two years. Initially, NYSTEC produced two foundation documents which were used by SysTest to aid in their understanding of what the scope of their testing should be. These included the New York State Requirements Matrix and the NYSTEC Security Testing Expectations document. Based on these documents, numerous joint meetings, conference calls and site visits, SysTest produced their NY State Board of Elections Voting System Verification Testing Master Test Plan document and the NY State Board of Elections Voting System Verification Testing Master Technical Data Package (TDP) Review Plan, which NYSTEC subsequently reviewed and recommended approval to NYSBOE. The SysTest testing effort was based on these foundation documents.

These foundation documents, which can be found on the NYSBOE website, are summarized below:

- New York State Requirements Matrix. This matrix identifies all VVSG, New York State voting system requirements, and provides a detailed breakdown of each requirement and where it should be tested in individual test cases. This document serves as a source document for verifying that all requirements were included in test cases and actually tested (Note: there is a separate matrix for each vendor).
- NYSTEC Security Testing Expectations. This document is a summary of multiple discussions at the beginning of the SysTest engagement dating back to January 2008. It provides an overview of testing expectations and provides examples of the level of detail expected in test cases.
- SysTest Labs Final Master Test Plan. This is the final SysTest Test Plan which was accepted by NYSBOE, after review by NYSTEC. This document detailed the specifics of how test plans would be constructed and what the contents would include. Included with this plan were sub-documents for the Technical Data Package Review (TDP) and related forms.

Once SysTest began drafting individual test cases, NYSTEC provided feedback in a variety of ways. During the development of the individual test cases, NYSTEC provided answers to SysTest questions related to clarification of individual requirements, testing methods, and the scope of the testing. As the individual test case development effort progressed, NYSTEC conducted multiple reviews of each test case as it was being drafted, providing feedback to SysTest on quality and content.

NYSTEC also participated in numerous conference calls to discuss requirements, and potential solutions with SysTest, both vendors, and NYSBOE prior to the commencement of testing. These discussions were used to assist voting system vendors and SysTest in understanding how their systems could be modified, when necessary to comply with requirements.

3. FUNCTIONAL AND SECURITY TEST CASES

Functional Testing, in general terms, refers to the non-security related VVSG and NYS requirements that focus on how the machines operate. Functional Testing included tests to determine if an election could be setup properly, if the machines allowed elections to be coded properly, and if all votes were cast and counted accurately.

Security related testing involves testing the voting systems against all security related requirements. These requirements are designed to evaluate the voting system's ability to provide confidentiality, integrity, availability, and accountability, while providing systems that will be usable. Additionally, security testing is designed to evaluate the system's ability to protect against tampering.

SysTest provided compensating controls and/or workarounds for all Functional Testing findings. NYSBOE is evaluating these compensating controls, and it is anticipated that they will be incorporated into revisions to NYSBOE's Policies and Procedures.

NYSTEC provided the compensating controls for the Security related findings commented on later in this report.

4. BACKGROUND ON SECURITY CONTROLS

4.1 Security Controls Overview

Electronic voting systems are a complex amalgamation of software, hardware, procedures, and security controls designed to ensure the confidentiality, integrity, availability, and privacy of an election are assured according to the law. Voting systems incorporate security controls to ensure that an election is conducted as mandated by law. These controls include management, operational, and technical safeguards or countermeasures that are provided by each vendor for use with their respective voting system. These controls — be they technical, operational (e.g. physical controls) or managerial (e.g. policy and procedural controls) — fall under the categories of prevention, detection or correction. They ensure that the voting system is not compromised or, if it is compromised, that the problems can be detected and corrective actions taken to ensure that the election proceeds unimpeded. These were the types of controls in the Voting Systems evaluated throughout the testing process.

4.2 Compensating Controls Overview

NYSTEC recommends that NYSBOE enact the proposed security compensating controls as part of NYSBOE's security-in-depth or security-in-layers approach to election security. There will never be a single security control that is always effective at mitigating risks. Security must rely on layers of controls because individual controls can and will fail. It is therefore necessary to implement several types of security controls which are defined in Appendix B. These compensating controls create additional layers of protection (as illustrated in Figure 1 Compensating Controls Supplementing Existing Voting Systems Controls) further mitigating security risks. Note that the risk is mitigated, not eliminated. This is because risk can never be totally eliminated in any complex system (especially those systems with significant involvement of human actors in a variety of roles) – it can only be mitigated to an acceptable level. Electronic voting systems are complex and involve the human actor to setup, administer, and use the systems. Mitigating the security risk associated with complex systems and their human actors is achieved through a varied and layered approach. If one control can be overcome, there will be another control that will compensate for that control's failure. Such an approach places additional obstacles for an attacker to overcome in order to compromise the election systems.

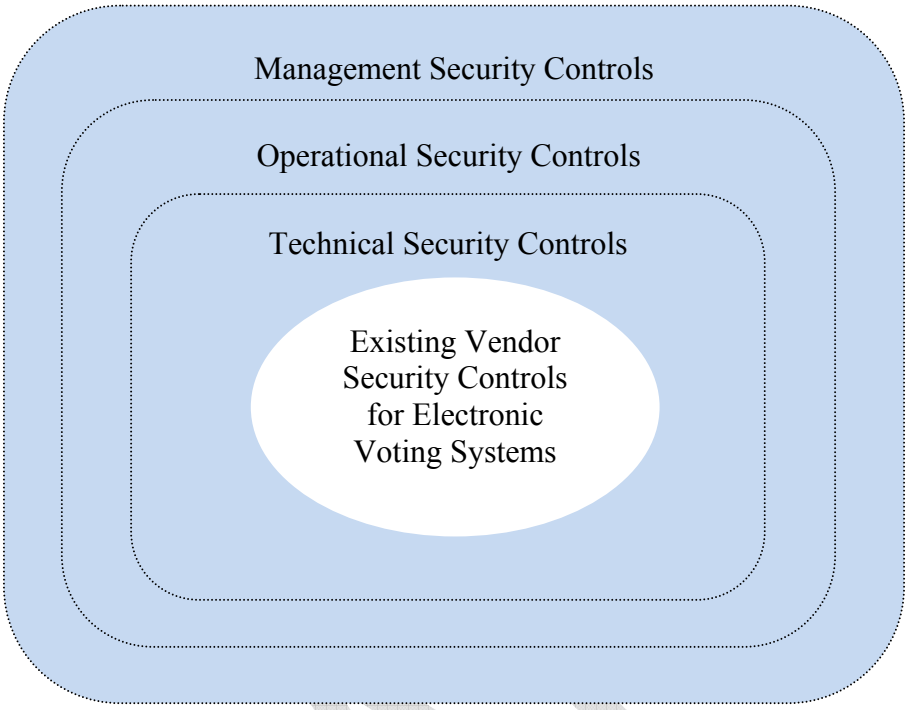

Figure 1 Compensating Controls Supplementing Existing Voting System Controls

Based on SysTest's findings for each voting system being tested, a set of compensating controls is recommended. Each presented control is part of a family of controls (see Appendix A) based on National Institute of Standards and Technology (NIST) SP800-53 groupings. Appendix B represents the actual compensating controls, along with their unique identifier and description. These control identifiers are used in Attachment A – Test Findings and Compensating Controls to associate a compensating control with the identified ITA findings.

4.3 Security Testing Findings

Security testing by SysTest revealed that while the vendors have implemented security sufficient to run an election, not all security requirements specified by Federal and NYS law were met in a wholly satisfactory manner. The findings are listed and described in Attachment A – Test Findings and Compensating Controls, along with their proposed compensatory security controls. This is the findings report delivered by SysTest for each vendor (Dominion and ES&S), supplemented by NYSTEC with compensatory security controls. The compensating controls, when implemented, will further strengthen the system and reduce the likelihood of a successful attack to compromise an election.

4.4 Discussion on individual Security Related Test Cases

4.4.1 Logical Access Controls Test Case

The objective of the Logical Access Controls test case was to determine whether the vendor has documented the logical access controls, and to verify the existence of the logical controls on the

voting system components. Examination was made on the types of roles defined and whether the roles were limited to particular election phases. Findings were chiefly due to the vendor not providing adequate policies for the logical access controls. There was a lack of documentation on whether roles were limited to a particular election phase or whether the role had rights in all phases of the election. In addition, the vendor did not document the points of attack and how logical access controls are used to mitigate these attacks. A set of compensating controls has been devised to mitigate the findings. For more information on the specific findings and compensating controls, see Attachment A – Test Findings and Compensating Controls.

The compensating controls implemented within the NYSBOE and CBOE policies and procedures will mitigate the various findings. Training must be aimed at ensuring that logical access controls are properly set up and maintained according to NYSBOE security policy and procedures for account and password management. Having properly trained personnel who follow policy and procedures is the first line of defense.

4.4.2 Physical Access Controls Test Case

The Physical Access Controls test case was designed to evaluate the physical security of the vendor-provided systems and their recommended security controls, such as locks, seals, and voter privacy. SysTest executed a test case using vendor-provided procedures and products to exercise all of these aspects of locks, seals, tamper evident controls, alarms, privacy screens, and other physical controls.

Most of the findings in this series of tests relate to ineffective seals recommended by the vendor and the lack of uniqueness of the physical keys. These findings can be resolved with the effective use of seals that have been evaluated by NYSBOE and recommended for use by the counties. Additional evaluations for the effective placement of seals and procedures for when they are removed were completed and have been provided to the counties.
As there were additional findings that were discovered during the testing of both vendor systems NYSTEC has provided compensating controls in order to best protect the use of the voting systems and the election outcome. For more information on the specific findings and compensating controls, see Attachment A – Test Findings and Compensating Controls.

4.4.3 Procedural Controls Test Case

The objective of the Procedural Controls test case was to determine whether the vendor has provided documented procedures to enforce security across the various components and election phases. Testing involved identifying the various documented security procedures, and then verifying the completeness and accuracy of those procedures against a system. Findings were chiefly due to the vendor not fully or accurately documenting a procedure; that is, the documented procedure did not match what the tester had to do or what the system was expecting. The vendors will be updating their documentation. Also, the vendors did not document the points of attack for each voting system component and the procedural controls in place to prevent an attack. A set of compensating controls have been devised to mitigate the findings. For more information on the specific findings and compensating controls, see Attachment A – Test Findings and Compensating Controls.

When the compensating controls are implemented into the NYSBOE and CBOE policies and procedures this will mitigate the risks associated with the various findings. Compensatory

controls, especially those aimed at the human element and specifically NYSBOE and CBOE policy and procedural controls, will need to be developed to address gaps in vendor policy and procedures across the various election phases. Compensating controls and proper training of CBOE personnel and poll workers will constitute the first line of defense when these machines are deployed.

4.4.4 Confidentiality Test Case

The objective of the Confidentiality test case was to test each system's ability to provide privacy to the voter and confidentiality of election data, where necessary, to ensure trust in the election process and in the results. Testing centered around confidentiality controls verifies how each system protects the voter's right to privacy both during and after an election. The test case was designed to ensure that no election processes or artifacts, such as audit logs or ballot images, could be used to determine how a voter voted. Additionally, the confidentiality testing included verifying that data was encrypted in real time, so interruptions to the system or failures such as a power loss did not leave data unencrypted.

Confidentiality testing was successful in determining if the data required to be encrypted was encrypted and identifying instances where voter privacy might have been compromised. Throughout the test campaign, each vendor was responsive to the NYSBOE provided list of data that should be encrypted and improved the overall security of their systems by implementing encryption controls on required data. Testing of both vendors' voting systems uncovered findings where the vendor did not adequately implement or document how the system uses encryption to protect against threats and how encryption keys are protected. NYSTEC recommends that counties use each vendor's system configured exactly the way it was when tested by SysTest.

Both vendors made considerable progress in the implementation of encryption. Where testing demonstrated issues, compensating controls, such as physical access controls, tamper evident seals, and improved county processes and procedures (such as room layouts) will enable the systems to be used safely. It is important to remember that no single compensating control will provide protections against findings around voting system confidentiality but rather the combined effect of layers of controls and processes.

Where the testing identified findings, there are associated compensating controls available to counties that will provide the necessary level of confidentiality. Results from this test case are closely tied to the results from the Crypto test case, where the cryptography behind the encryption was examined.

4.4.5 Integrity Test Case

The objective of the Integrity test case was to test the system from an integrity aspect against all relevant security requirements. Integrity requirements are focused on the ability of the system to provide trust in the validity, accuracy, and authenticity of the election, data, and artifacts. This is accomplished by providing protection against unauthorized modifications to election data and the detection of any event that could impact the accuracy of, or trust in, the election results. This

test case was designed to focus heavily on the use of digital signatures as required by NYS Election Law, as well as other security provisions contained within the system that provide data authenticity and integrity. The testing was designed to focus on where integrity controls are present and how effective they are. In particular, the testing looked at the effective use of digital signatures in key places such as removable media, ballot records and images, audit logs, and election databases. The test case was designed to evaluate all controls claimed by the vendor from both a functional testing and code review standpoint. Results from this test case are closely tied to the results from the Crypto test case, where the cryptography behind the digital signatures was examined.

Testing of both vendors' voting systems uncovered findings where the vendor did not adequately implement or document how the system uses digital signatures to protect against threats. The documentation did not address how public and private keys were managed and this, combined with the testing for FIPS compliance in the Cryptographic test case, led NYSTEC to make numerous recommendations on compensating controls to augment the protections provided by digital signatures. NYSTEC recommends that counties use each vendor's system in the manner in which it was configured and tested by SysTest. Both vendors were successful in implementing digital signatures to a point where they do provide detection of tampering with election data. The presence and effectiveness of digital signatures was tested on critical components such as election databases, audit logs, election results, and removable media files. Due to the importance of data integrity within the EMS systems, specifically databases, NYSTEC is recommending the use of disk encryption or similar methods as an additional preventative control to add additional integrity controls. Specific discrepancies can be found in each vendor's attached finding reports, along with compensating controls. Integrity testing also tested the ability of the system to preserve election results when errors such as power loss and memory failures occur. The results here demonstrated cases where the system was unable to completely recover.

These findings again highlight the importance of sound voting system procedures to be able to respond to such conditions and have influenced the NYSTEC list of compensating controls. Both vendors made considerable progress in the implementation of digital signatures and where testing demonstrated issues, compensating controls such as physical access controls and tamper evident seals will enable the systems to be used. It is important to remember that no single compensating control will provide complete protection against findings around voting system integrity; rather the combined effect of layers of controls and processes is required.

4.4.6 Accountability Test Case

The Accountability test case was designed to test that the Voting Systems can allow election officials to determine all the events that occurred in the system for an election. This enables election officials to ensure the election was created and ran correctly, and to help understand what went wrong, if errors should occur. From a practical standpoint, this means the test case tests the auditing capabilities of the system to see that all important events are logged and that the system protects the integrity of those logs.

The findings against both vendors are generally issues about being able to alter audit logs. Fortunately, physical controls on the scanner and Ballot Marking Device (BMD), procedural controls on the handling of the memory devices after an election, and logical access controls on Operating System logging on the EMS, can mitigate that risk of manipulating the log data.

4.4.7 Availability Test Case

The Availability test case was designed to test the Voting Systems' ability to be available when needed in the election process. These tests verify that the systems are resilient against failures and can recover from failures without corrupting data.

Both vendors had findings about the BMD still operating when it had ink cartridge issues. These can be mitigated by proper procedures before transport to polling places to ensure the devices have enough consumables and are working properly. There were also some issues of not logging the errors when a memory or power failure occurred. These can be compensated by well-trained poll workers and a well-defined incident response process whereby if a poll worker notices any anomalies in the use of the system (i.e. unexpected behavior from the devices) the proper persons get notified so they can ascertain what happened and make decisions on whether mitigation procedures should be invoked (such as manual count of ballots).

It is important to note that there is no way to completely eliminate the risk of a catastrophic system failure, so it is very important to have procedures in place to backup and restore EMS data, as well as procedures to use emergency ballots at polling sites. The BMDs and Scanners have built-in backup power, but the EMS servers and workstations do not. Therefore, NYSTEC recommends that these devices use an uninterruptable power supply (UPS) to ensure that if there is a power failure when the machines are in use, no damage will be done to the machines or the data.

4.4.8 Threat Resistance Test Case

The Threat Resistance security test case was designed to evaluate the security controls of the vendor-provided systems against know vulnerabilities found in the requirement matrix. SysTest executed a test case to determine whether the vendor built sufficient security controls into the system to provide a secure environment.

The NYSTEC recommended compensating controls are sufficient to mitigate risks identified in this test case.

4.4.9 Operating System Hardening Test Case

The overall objective of the Operating System (OS) Hardening test case is to test both the security controls claimed by the vendor to be incorporated in the Operating System of the EMS computer(s), BMD and Scanner, and to ensure that the Operating System itself is locked down so it is not subject to any vulnerabilities to the system. It also tests any other security software that is installed (such as Anti-Malware and Firewalls).

The most important test is one whereby a benchmark configuration is used as a checklist to compare to the configuration of the Operating Systems of the election system devices. SysTest chose the Federal Desktop Core Configuration for all Workstations and servers using Windows XP or Vista and the National Checklist Program Repository for other OS as needed http://web.nvd.nist.gov/view/ncp/repository. Both vendors had failures in the comparison of the benchmark to their OS hardening. However, at a high level, it is important to note that any failures or vulnerabilities found in the EMS OS Hardening are compensated by the fact that the complete EMS system (servers, workstations, and closed networking equipment) will have stringent physical access controls so that only authorized personnel can physically access the devices at all. The scanners and BMDs will also have physical access controls while in storage

and transit. Moreover, access to the operating system itself on the scanners and BMDs involves many steps, including access to internal components of the device. Direct access to the operating system cannot be made from the standard interfaces of the devices (which only access the voting system software itself).

4.4.10 Trusted Build Test Case

The Trusted Build test case was designed to ensure that all vendor-developed software could be compiled from its source form into binaries in a controlled and trusted environment. This trusted build environment was built by SysTest and used to compile and build the software images that were subsequently used to install software on each of the voting system components under test. All of the trusted build work was done at the SysTest site under supervision of NYSBOE and NYSTEC. In addition to performing the build, several requirements related to SysTest acting in the capacity as the National Software Release Library (NSRL) were validated. This included the generation of hash values for all modules to be used as criteria for the software validation by CBOEs. The trusted build test case generated a large amount of artifacts, including all steps taken in the build, as well as information and the processes used to ensure that all 3rd party and COTS software were derived from their original and authoritative sources

4.4.11 Crypto Test Case

The Cryptography test case was designed to validate that all cryptographic functions present within the voting system were derived from cryptographic modules that have been approved for use by the NIST Cryptographic Module Validation Program (CVMP). This program validates cryptographic modules to Federal Information Processing Standards (FIPS) 140-2 Security Requirements for Cryptographic Modules. Cryptography is one of the more challenging areas of computer programming, and the use of FIPS modules according to specific security policies ensures that functions such as hashing, encryption, and the use of digital signatures are implemented in the most secure manner. This test case used documentation and code review, as well as functional testing, to identify all cryptographic functions used within each voting system. Then, through code review and compliance with mandatory security policies, the test case determined if all cryptography present in the voting system was in fact FIPS compliant.

Achieving FIPS compliance involves using the appropriate cryptographic algorithms and implementing them properly within the software. Testing results show that while both vendors attempted FIPS compliance, neither used FIPS validated modules in all cases. Where they did use the modules, they were not always implemented properly. It is important to note that using only FIPS validated modules in the prescribed manner is certainly the goal, as this means all aspects of cryptographic functions were implemented properly, including the very important aspect of key management. Even though neither vendor used only FIPS compliant modules, this does not mean the encryption and digital signatures used are not very effective in providing security benefits. Early in the testing effort, neither vendor made extensive use of encryption or digital signatures, and prior to testing, both vendors made considerable gains in implementing digital signatures and encryption as specified in NYS requirements. As can be seen in the detailed testing results, both vendors for the most part used FIPS compliant algorithms, which is the first step to being fully compliant.

When used in combination with the compensating controls recommended by NYSTEC for each vendor (see appendices), the implementation of cryptographic functions supporting the

encryption and digital signature functions within the voting system will provide the protection necessary to utilize the voting systems in a secure manner. Each vendor should continue to strive to achieve FIPS compliance, as doing so will enable some of the compensating controls to be relaxed. Because of the lack of FIPS compliance by both vendors, especially in the area of key management and use of some cryptographic functions, compensating controls will include strict chain of custody rules, as well as physical controls such as locks and tamper evident seals.

4.4.12 Source Code

An analysis of the source code review was completed by a NYSTEC subcontractor (SRA/REBA) that specializes in code review and evaluations. That report is included as Attachment B – SRA/REBA Source Code Review. All source code findings have been mapped to compensating controls in Attachment A – Test Findings and Compensating Controls

4.4.13 Telcom Test Case

The Telecom security test case was primarily designed to determine if the voting systems are in compliance with NYS law, which requires that voting systems not have networking capabilities. SysTest executed a test case that evaluated if all networking capabilities, both hardware and software, have been disabled for the systems under test.

No findings are directly associated with this test case, as all requirements were tested in other test cases. When findings were indicated in other test cases, NYSTEC provided compensating controls for the findings in the other test cases. For details, please refer to the vendor specific attachment to this report for pointers to the other test cases.

5. APPENDIX A

Identifier NYS identifier used for mapping to discrepancies.	**Family** Category of compensating control	**Class** Classes based on dominate characteristics of controls within the family.
AC-NYS	Access Control	Technical
AT-NYS	Awareness and Training	Operational
AU-NYS	Audit and Accountability	Technical
CA-NYS	Certification, Accreditation, and Security Assessments	Management
CM-NYS	Configuration Management	Operational
CP-NYS	Contingency Planning	Operational
IA-NYS	Identification and Authentication	Technical
IR-NYS	Incident Response	Operational
MA-NYS	Maintenance	Operational
MP-NYS	Media Protection	Operational
PE-NYS	Physical and Environmental Protection	Operational
PR-NYS	Procedures and Planning	Management
PS-NYS	Personnel Security	Operational
RI-NYS	Risk Assessment	Management
SA-NYS	System and Services Acquisition	Management
SC-NYS	System and Communications Protection	Technical
SI-NYS	System and Information Integrity	Operational
The above table is largely based on NIST SP800-53 Recommended Security Controls for Federal Information Systems.		

6. APPENDIX B

Compensating Control ID	Compensating Control Name	Description	*Comments*
AC-NYS1	Proper Account Management and Usage	System shall have a unique administrator (split password) account that is not used for elections processing. All other accounts are granted only the access level necessary to complete tasks. Users are assigned to appropriate roles and accounts to provide support for separation of duties and need-to-know.	*The proper use of accounts and roles ensures that election workers are granted only enough privilege to do their jobs.*
AT-NYS1	Properly Trained Poll Workers	Poll workers have completed basic training and understand their roles and responsibilities	*The weakest link in security is always the human link. Properly trained poll workers is vital to being able to detect problems or suspicious behavior and knowing how to respond.*
AT-NYS2	Properly Trained CBOE workers	CBOE staff have been properly trained and understand their roles and responsibilities.	*The weakest link in security is always the human link. Properly trained staff will identify problems and know how to respond to them. Flaws in voting system software will always exist and well trained CBOE staff will be needed to report the issues and improve the overall quality of the system over time.*
CA-NYS1	County BOE Security Assessments	Regular assessments of County implementation of NYSBOE Policies and Procedures	*Necessary to ensure CBOEs are implementing all the necessary mitigating controls to safely use the systems. The audits should be conducted to determine how well the NYSBOE Policies and Procedures are being followed. Of course each CBOE will fine tune procedures to fit their environments.*
CM-NYS1	Configuration Management	Configuration management as per NYSBOE Policies and Procedures.	*Configuration management is the proper management of the voting systems to ensure that all systems are running only the proper versions of software and no unauthorized software which could exploit vulnerabilities on the system. Proper configuration management is possible when all NYSBOE policies and procedures are in place.*

Compensating Control ID	Compensating Control Name	Description	*Comments*
CM-NYS2	Hardening of EMS systems as per vendor specifications	County EMS systems have been hardened as per vendor instructions.	*Hardening is the removal of all unnecessary software and the validation that security settings are configured properly. CBOE EMS systems to be hardened as per vendor procedures. As vendors update hardening documentation these procedures will be reviewed and tested as necessary.*
CP-NYS1	Emergency Ballots	Use of emergency ballots and corresponding emergency procedures	*Ability to continue voting despite any problems with the voting system is a key property of paper based systems. Documented procedures in this area will provide for a smooth transition to emergency ballots.*
IA-NSY1	Authenticated Actions	Use of all required system authentication controls in the desired manner. No sharing of accounts and passwords.	*Auditibility and proper access controls is only possible when all users are required to authenticate and accounts are never shared.*
IA-NYS2	Account and password management	Proper administration of voting system accounts based on roles. Proper use of passwords. Use of accounts and passwords as per NYSBOE Policies and Procedures	
IR-NYS1	Incident Response Plan for voting system tampering or problems	In the event of suspected tampering a process is in place to determine impact and resolution	*The Incident Response plan will help in providing a controlled response to any potential incident.*
MA-NYS1	Voting System Maintenance	Voting systems are maintained in a manner that ensures that they are always the correct current certified version and comply with NYSBOE Voting System Security Policy and Procedures	*Proper maintenance as per NYSBOE regulations, policies and procedures ensure systems remain in the certified state.*
PE-NYS1	Tamper Evident Seals	Effective use of high quality tamper evident seals as per security procedures.	*This is necessary to enable CBOEs to procure effective seals as the seals are a key layer of security and therefore must be effective in providing tamper detection.*
PE-NYS2	UPS for EMS Systems	Use of Uninterruptable Power Source (UPS) on CBOE EMS systems	*Testing identified loss of power as having potential for loss of data. UPS could save many hours of work and is an excellent preventative control and provides a compensating control for several of the functional findings.*
PR-NYS1	Paper ballot chain of custody	Strict adherence to the polling place paper ballot chain of custody requirements as specified in NYSBOE Voting System Security Policy and Procedures	*Important to be able to detect known vulnerabilities such as ballot stuffing.*
PR-NYS2	Poll Workers Procedures	NYSBOE Voting System Procedures updated to include all potential error messages and corresponding	*Poll worker procedures should include that the poll worker periodically verifying the voting*

Compensating Control ID	Compensating Control Name	Description	*Comments*
		actions.	*system seals and counters.*
PR-NYS3	Pre Qualification Test Procedure	Describes the activities performed by CBOE during election preparation and planning. Overview: (Dry Run and Run for Record) • Create Election Configuration • Conduct voting system inventory • Create Ballot Configuration • Create PDF for each ED • Proof each ED • Send proof to printer • Verify printed proof • Perform hash check • Scan printed proof to verify correctness • Create test decks • Create removable media • Inspect each voting system • Re-calibrate voting system • Run test deck in election mode • Verify results • Copy files for 24 month storage retention • Attach security seals • Prepare voting systems for shipment	*Where possible CBOE's should consider not allowing media to sit in systems overnight. As systems will not be monitored once delivered to poll places, it is critical that all security measures are strictly adhered to prevent unauthorized access.*

Compensating Control ID	Compensating Control Name	Description	*Comments*
PR-NYS4	Post Election Poll Site Procedure	Describes the activities performed at the poll site after the close of polls. • Secure poll site • Verify security seals are intact • Close poll • Print results tape • Record public and protective counters • Inspectors sign results tape • Affix tape to canvass statement • Power down scanner • Account for all ballots • Announce votes cast from reports tape • Canvas emergency, absentee, military and special ballots • Store affidavit ballots • Store all ballots in secure container • Remove 1 memory device and place in secure container • Re-attach security seals • Record all security seal serial numbers • Complete canvass statement • Inventory supplies • Attach and verify all security seals • Document chain of custody • File returns to CBOE	
PR-NYS5	Quarterly Maintenance Test Procedure	Describes the activities performed by CBOE during a non-election quarter. • Verify Security Seals • Perform Hash Check if Appropriate • Create test deck • Inspect voting system for damage • Run test deck in election mode • Verify results • Copy files for 24 month storage retention • Update interim asset management spreadsheet • Attach security seals • Ready voting system for storage • Verify results using EMS (optional)	
PR-NYS6	County Receipt Procedure	Describes the activities performed by SBOE, the voting system vendor and CBOE for the initial delivery of voting systems to the CBOE facility.	

Compensating Control ID	Compensating Control Name	Description	*Comments*
PR-NYS7	Restoration of Chain of Custody Procedure	Describes the activities performed by CBOE when the voting system has been outside their chain of custody (i.e., sent to the vendor for repair, loaned to a school board, etc…) • Coordinate return of voting systems from 3rd party • Unpack voting system • Verify security seal • Verify inventory • Inspect voting system for damage • Conduct software validation (hash check) • Verify voting system functionality • Attach and record security seals • Ready voting system for storage	
PR-NYS8	Test Deck Procedure	Describes the activities performed in preparing a test deck. Types of test decks: • Acceptance Testing (standard or comprehensive) • Pre-Qualification Testing (standard or comprehensive) • Maintenance (standard)	
PR-NYS9	Election Information Control and Archiving Procedure	The procedures used by the CBOE to maintain a chain of custody of all voting related materials and media, before, during, and post election	*Election artifacts, both electronic and paper should be secured and stored as per Election Law requirements.*
PR-NYS10	Change Management Procedure	The NYSBOE and CBOE procedures that need to be followed for any changes to hardware or software on the election systems.	*This ensures that voting systems are only used for elections and any software or hardware changes are certified and delivered by NYSBOE for the Counties.*
PR-NYS11	Incident Response Procedure	The procedures to be followed by poll workers and CBOE personnel in the event of an incident affecting voting. Incidents can be manmade or natural disasters, etc	*Critical process that is necessary to control elections when problems occur.*
PR-NYS12	Disaster Recovery Procedure	The procedures used by the CBOE to proceed with voting in the event of or the aftermath of a natural disaster.	
PR-NYS13	Voting Systems Administration Procedure	These procedures document how the CBOE maintains the system and fills in any gaps that exist within the vendor documentation. The procedures should be expanded to incorporate the necessary controls around physical access, closed network, system hardening, dedicated usage and Need-to know	*Vendor documents are supplemented by NYSBOE procedures.*

Compensating Control ID	Compensating Control Name	Description	*Comments*
		for individuals.	
PR-NYS14	Software Validation Procedure	Use of voting system software validation tools (hash checks) as per NYSBOE Policies and Procedures to ensure system is free of uncertified software or firmware.	
PR-NYS15	CBOE Voting Systems Usage Procedure	CBOE use of systems as per mandatory security controls and for proper use of closed networks.	
PR-NYS16	Election Day Poll Site Procedure	Describes the activities performed at the poll site. • Setup voting area • Verify security seals • Unpack voting system • Check supplies • Account for ballots • Inspect voting system • Inspect ballot compartments • Attach security seals • Open polls • Print Zero Report tape • Monitor security seals	
PR-NYS17	Room Power and Storage Procedure	This document will serve as an operational guide for counties. The topics in this guide provide examples and best practices gathered from voting system manufacturers, other states and the Election Assistance Commission (EAC). The State Board will continue to search for best practices and tested procedures which can be implemented by county boards of elections throughout New York, and will provide same to County Boards, regularly. Overview: • Voting system facility • Polling place guidelines • Voting system delivery	
PR-NYS18	Removed as redundant with other compensating controls		

Compensating Control ID	Compensating Control Name	Description	*Comments*
PR-NYS19	Acceptance Testing Warehouse Procedures	Describes the activities performed by NYSBOE, the voting system vendor and SBOE during the acceptance testing process. • Inspect Voting Systems for Damage • Conduct Inventory of Voting Systems • Assign to County and Random Select Voting Systems for Comprehensive Test • Conduct Hash Check • Perform Functional Test (Standard or Comprehensive) o Key points: o System Diagnostics o Print Zero Report Tape o Scan ballots to verify: § proper messages are displayed § optical scanner distinguishes EDs § votes are tallied correctly o Print Close Poll Report Tape • Attach Security Seals • Return Voting Systems to Vendor for Shipment to CBOEs	
PR-NYS20	County Receipt Procedure	Describes the activities performed by SBOE, the voting system vendor and CBOE for the initial delivery of voting systems to the CBOE facility. • Verify Security Seals • Verify Inventory • Inspect Voting System for Damage • Verify Voting System Functionality • Attach Security Seals • Ready Voting System for Storage	
PR-NYS21	Audit Procedure for 6210.18	Describes the activities performed when conducting the 3% audit per 6210.18.	

Compensating Control ID	Compensating Control Name	Description	*Comments*
PR-NYS22	Voting System Certification	Describes the SBOE voting system certification process. • Voting machine application for certification • Application requirements • State Board of Election Polices on processing applications • Accounting practices for vendor testing account by the state board • State board to acquire ITA • Technical data package review • Master test plan submission requirements • Individual test plan creation • Usability test plan creation • Security test plan • Testing of voting system • Functional testing of voting systems • Voting system certification • Recertification	
PR-NYS23	Physical Key Chain of Custody	Procedure to provide strict chain of custody of physical keys (including iButtons) during election phases.	*NYSBOE and/or CBOEs will own and securely maintain all admin keys and passwords.*
PR-NYS24	Manual Count of Paper Ballots	Hand count of ballots in the event of a system failure	
PR-NYS25	NYSBOE Security Policy	NYSBOE Voting System Security will supplement vendor documentation	
PR-NYS26	NYSBOE Emergency Update Approval Procedure	NYSBOE procedure and process to provide a rapid assessment of vendor patches and approval for use on voting systems prior to re-testing and re-certification.	
PS-NYS1	Job Rotation	BOE jobs are rotated each election.	*Where possible CBOE's should rotate staff occasionally between various election roles as this improves the changes of identifying inappropriate insider activities.*

7. ATTACHMENT A – TEST FINDINGS AND COMPENSATING CONTROLS

7.1 DOM_Findings_Report-NYSTEC Compensating Controls (FINAL DRAFT 12-11-2009)

7.2 ESS_Findings_Report-NYSTEC Compensating Controls (FINAL DRAFT 12-11-2009)

8. ATTACHMENT B – SRA/REBA SOURCE CODE REVIEW

8.1 SRA_REBA_code_review_Dominion_final

8.2 SRA_REBA_code_review_ESS_final