New York State Technology Enterprise Corporation

NYSTEC Review of SysTest Master Test Plan and Supporting Documents

New York State Board of Elections

Submitted to:

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

April 23, 2008
Version 1

Table of Contents

1. REVIEW OF SYSTEST MASTER TEST PLAN

The NYS Board of Elections requested NYSTEC to complete a review of the SysTest "NY ITA Master Test Plan Rev 1.0.doc".

The Master Test Plan (Master Test Plan) also includes the following attachments that were included as part of the review:

1. "NYS Voting NYSBOE LOT 1 Systems Master Requirements Matrix Rev1.0.xls"
2. "NY ITA Master TDP Review Plan Rev 1.0.doc"

We were pleased to see that much of the content from previous discussions, the testing expectations document, and the requirements matrix were included in these documents. Over the last few months, at SBOE request, NYSTEC and SysTest have held a number of joint working sessions in an attempt to clarify expectations and work out a mutually acceptable approach to the planning and testing process. We believe this was "time well spent" and is reflected positively in these documents.

Overall NYSTEC feels that the test plans, requirements matrix and TDP Review Plan have improved considerably from earlier versions and will be acceptable after SysTest provides final versions with the revisions suggested later in this document. It is anticipated that our comments will be reviewed by SysTest and if any of these comments are unclear or disputed by SysTest they will provide feedback so that we can jointly work out an acceptable solution. We are confident that with a concentrated effort on revisions this process can be accomplished by the May 1st deadline.

The documents reviewed are the beginning process in preparing for voting system testing however, the true test will be in SysTest's ability to map each requirement to a machine specific test procedure that accomplishes the objectives detailed in the NYSTEC Security Testing Expectations document.

In order to facilitate this review we have "inserted comments" within the specific documents (With the exception of the requirements matrix) that should be reviewed by SysTest and used to make revisions to these documents. In addition to the comments that are within the documents we have included significant high level comments in the following sections. These high level comments are supported by similar comments within the documents and should be referenced for clarification.

2. GLOBAL OR HIGH LEVEL FINDINGS

The following are high level findings that are general or global to all documents:

- New York State law and regulations requires that all requirements be tested. In order to facilitate that requirement the official "Run for Record" is designed to ensure that ALL tests are completed for all requirements after the vendor has provided fixes for any discrepancies found during the break/fix phase of testing. SysTest has indicated that a subset of tests, but not less than 80% of the tests, will be completed during the "Run for Record". This is considered unacceptable as ALL tests must be run, following the final witness build, during this process. If tests will not be run they must be documented with valid reasons for not running them.

- There are many references to evaluating prior work in both test plans to determine what can be re-used in future testing. Some caution is required to ensure that any prior testing that is used meets a critical requirement that it is from a "significantly similar" system. Since this is a subjective criterion some guidelines need to be defined to make this objective. For example, a comparison of hash values could be done. In other places SysTest states that prior state and ITA work will be evaluated to help them construct good test cases and to ensure that vulnerabilities identified in prior testing are resolved. This use of prior test results is excellent and encouraged.
- The Final Test Report is referenced in both plans but with minimal definition of the content and format. The format and content of this report is critical and should be designed and approved by the SBOE well in advance of finalizing it. NYSTEC has suggested that the requirements matrix be used as the foundation for the Final Test Report with the addition of three columns for the test date, tester initials and observer initials.

3. FINDINGS FOR SPECIFIC DOCUMENTS

The following are high level findings that are specific to each document incorporated in the Master Test Plan:

3.1 Findings in "NY ITA Master Test Plan Rev 1.0.doc"

- Mapping to the test cases and steps need to be completed.
- There is a test case that is designed to test that all functions of communications are effective and safe. However, NYS requirements forbid the use of external communications and all communications tests should be designed to ensure they can not communicate.
- Consistently throughout the document references are made that these tests are run to ensure the vendor "meets" the requirement. The tests in fact are to determine which requirements they pass or fail. This is different than EAC testing as that process was developed to assist the vendor in receiving a certification. This is critical to understand since there is no time in the schedule to keep testing until all discrepancies are fixed.
- Test case – General – Table number 20 is just a rehash of what will be tested and should be revised to indicate "how" the requirements will be tested.
- See 3.3 below for additional findings related to the quality of the test cases contained within the Master Test Plan.

3.2 Findings in "NY ITA Master TDP Review Plan Rev 1.0.doc"

- Wherever there is a reference to COTS or Source Code to be reviewed the "NYSBOE Certified Voting System Escrow Requirements – Final" document needs to be referenced for definition purposes.
- Although there are already some references to regression testing, additional references to the actual Systest regression test plan needs to be made throughout the document where indicated in file.
- Systest lists the use of numerous code analysis tools in the plan, but only prescribes the use of one in other documents.

- Much of Appendix A (pages 56-126) is essentially a rehash of the VVSG requirements into groups that adds little value to the plan as this is already done in the Requirements Matrix.

3.3 Findings in "NYS Voting NYSBOE LOT 1 Systems Master Requirements Matrix Rev1.0.xls"

General Comments

The primary goal of the requirements matrix was to create a working and public document that would help ensure the following:

- ITA has identified all requirements that must be tested in NYS.
- ITA shows an understanding of the requirements by documenting at a high level how the requirement would be tested. This could be accomplished by describing the test method within the matrix, or by referencing the appropriate test case or cases within the Master Test Plan (Master Test Plan), or a combination of both.
- The ITA included an emphasis on security testing by including negative testing and an emphasis on source code review beyond what was done in prior ITA certifications.
- That NYS does not find itself in the position that other states are in when certified voting systems are found to contain numerous vulnerabilities that were not identified during the certification process.

NYSTEC feels that SysTest does understand the higher level to which NYS testing must be held and is in agreement with us on which requirements have elements of source code review and are security related. This is evident through the numerous conversations and working sessions NYSTEC and SysTest completed and by how the requirements are marked (security and source code related) within the matrix. NYSTEC believes that the Security Specialists, Functional Specialists and leads within SysTest fully understand this and are working to accomplish it.

Where we feel there is significant improvement needed, based on the recently delivered Requirements Matrix and Master Test Plan is in the mapping of requirements from the matrix to the test cases in the Master Test Plan. For the majority of requirements there are comments to describe the approach that will be taken which is good, but there are generally no mappings to test cases within the Master Test Plan. Additionally the test cases in the Master Test Plan need work if Systest is to successfully link each requirement to the appropriate test cases. Detailed findings that support this conclusion are below in the detailed comments section.

Detailed Comments

1) Security Source Code Validation column comments need a quality review

For many requirements in the matrix that are marked as security related and in need of a functional and/or security focused review SysTest used the following to describe how the testing would be done:

"*Security source code review focuses on a large number of security vulnerabilities as documented in "Table 7 - Areas of Security Focused Source Code Review" of the "Master Technical Data Package Review Plan".*

Any of these vulnerabilities existing in code applicable to this requirement will be detected by Fortify SCA and reviewed manually."

The first problem is that SysTest used this exact text more than 600 times to describe how testing would be accomplished. This tends to jump out at the reader and demonstrates an overly simplistic view of how to accomplish source code testing.

The second and more concerning finding is that SysTest seems to believe that Fortify will find all vulnerabilities related to 600+ requirements, which of course it, or any other code analysis software will not do. SysTest needs to use a combination of code analysis tools and manual code review combined with functional testing to ensure that a machine is properly tested against given requirements. The requirements matrix comments need to be reviewed for quality and more detail should be added there or in the test cases (when mapping happens) that help ensure that resulting test procedures and machine specific test cases are consistent and of high quality.

2) Test case mappings are largely incomplete and where they are populated map to steps that do not exist in test cases in the Master Test Plan.

One of the goals of the requirements matrix was to map each requirement to the test case or test cases that will be followed to build machine specific test cases. This task is largely incomplete. In the Master Test Plan there are test cases that are not identified in the matrix (namely the security ones). The purpose of the mapping goal is to help ensure that system specific test cases are constructed in similar fashion and with similar focus to ensure fair and thorough testing of each machine. SysTest will have a significant amount of work to create these mappings as they are also concurrently developing and improving the test cases within the Master Test Plan.

3) Concern over mapping so many requirement to so few test cases.

NYSTEC has expressed a concern in the past over how large and complex test cases will become when some 2000+ requirements are mapped to approximately 12 test cases. Where tests cases become too long and not well focused NYSTEC suggests that SysTest consider creating additional test cases. Additionally, most of the test cases involve exercising the machine as if it were running an election. NYSTEC suggests that SysTest consider other non-election driven test cases for security testing as well as negative testing. The best way to validate a vendor's claim may not be to run the system in the prescribed manner but rather as an attacker would access the system.

4) Functional comments are generally more complete and well thought out

NYSTEC found that throughout the matrix the functional test comments had more detail and the author seemed to understand the type of functional test that would compliment a source code review or stand alone where only a functional test was needed. Still, throughout the matrix, there are instances where the tester is validating the requirement by referencing vendor statements in the TDP. This should never be enough validation to pass a requirement. In these cases the test case should seek to corroborate the vendor documentation with functional tests and source code review as needed. Again, NYSTEC saw a better job of this in the functional comments however we continue to stress the importance of the functional testers and source code reviewers working closely together as needed where requirements need to be tested through multiple forms of testing.